

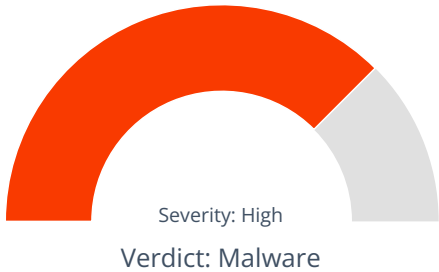
Summary

File Name: Servidor.exe
File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1: 96ee36b80ad6918ccd1e5568ab9522c27cdeced7
MD5: 1ba88acd9206b22b8b55e903f86db7b6

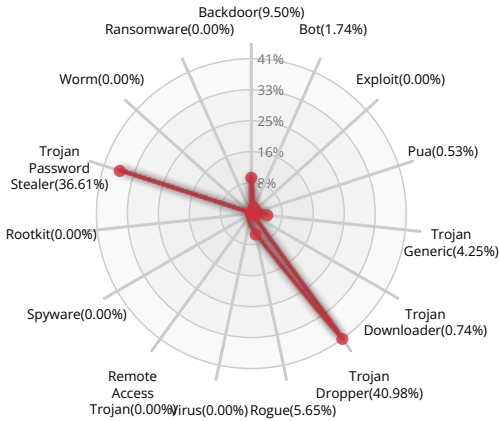

MALWARE

Valkyrie Final Verdict

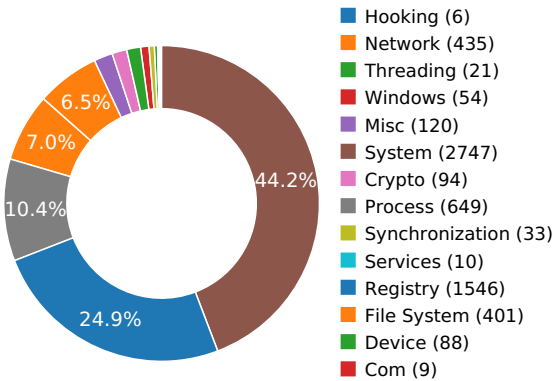
DETECTION SECTION



CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Networking	1	(16.67%)
Stealing of Sensitive Information	1	(16.67%)
Hooking and other Techniques for Hiding Protection	1	(16.67%)
Data Obfuscation	1	(16.67%)
Persistence and Installation Behavior	1	(16.67%)
Malware Analysis System Evasion	1	(16.67%)

Activity Details

NETWORKING



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

Show sources

STEALING OF SENSITIVE INFORMATION



Sniffs keystrokes

Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION



Creates RWX memory

Show sources

DATA OBFUSCATION



Drops a binary and executes it

Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR



Creates a copy of itself

Show sources

MALWARE ANALYSIS SYSTEM EVASION



A process attempted to delay the analysis task.

Show sources

Behavior Graph

15:49:08

15:50:48

15:52:28

PID 2300

15:49:08

Create Process

The malicious file created a child process as 96ee36b80ad6918ccd1e5568ab9522c27cdec7.exe (**PPID 2244**)

15:49:08

NtAllocateVirtualMem

PID 2436

15:49:08

Create Process

The malicious file created a child process as server.exe (**PPID 2300**)

15:49:08

NtDelayExecution

15:49:11

Create Process

15:49:16

GetAsyncKeyState

15:49:23

15:52:28

WSAConnect

[53 times]

PID 2564

15:49:12

Create Process

The malicious file created a child process as netsh.exe (**PPID 2436**)

Behavior Summary

ACCESSED FILES

C:\Windows\System32\MSCOREE.DLL.local
C:\Windows\System32\tzres.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll
C:\Windows\Microsoft.NET\Framework*
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorlib.dll
C:\Program Files\Common Files\System\sysmrv.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorlib.dll
C:\Users\user\AppData\Local\Temp\A1D26E2
C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
C:\Users\user\AppData\Local\Temp\96ee36b80ad6918ccd1e5568ab9522c27cdec7.exe.config
C:\Users\user\AppData\Local\Temp\96ee36b80ad6918ccd1e5568ab9522c27cdec7.exe
C:\Users\user\AppData\Local\Temp\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\system\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\ProgramData\Oracle\Java\javapath\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\wbem\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\Python27\Scripts\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\sysinternals\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\api-ms-win-appmodel-runtime-l1-1-0.dll
C:\tools\IDA_Pro_v6\python\api-ms-win-appmodel-runtime-l1-1-0.dll

C:\Users\user\AppData\Local\Temp\96ee36b80ad6918ccd1e5568ab9522c27cdec7.exe.Local\
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
C:\Windows
C:\Windows\winsxs
C:\Windows\Microsoft.NET\Framework\v4.0.30319
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\fusion.localgac
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index12a.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.INI
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\ole32.dll
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\96ee36b80ad6918ccd1e5568ab9522c27cdec7.config
C:\Users\user\AppData\Local\Temp\96ee36b80ad6918ccd1e5568ab9522c27cdec7.INI
C:\Windows\System32\intl.nls
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\GAC\PublisherPolicy.tme
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.INI
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBasic#\08d608378aa405adc844f3cf36974b8c\Microsoft.VisualBasic.ni.dll
C:\Windows\assembly\GAC_MSIL\Microsoft.VisualBasic\8.0.0.0__b03f5f7f11d50a3a\Microsoft.VisualBasic.INI
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\dbfe8642a8ed7b2b103ad28e0c96418a\System.Drawing.ni.dll

C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\3afcd5168c7a6cb02eab99d7fd71e102\System.Windows.Forms.ni.dll

C:\Windows\assembly\GAC_MSIL\System.Windows.Forms\2.0.0.0__b77a5c561934e089\System.Windows.Forms.INI

C:\Windows\assembly\GAC_MSIL\System.Drawing\2.0.0.0__b03f5f7f11d50a3a\System.Drawing.INI

C:\Windows\Globalization\en-us.nlp

C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp

C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp

C:\Users\user\Desktop\server.exe

C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\shell32.dll

\\?\MountPointManager

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NETFramework\InstallRoot

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

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NETFramework\CLRLoadLogDir

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\NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NETFramework\OnlyUseLatestCLR

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NETFramework\GCStressStart

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NETFramework\GCStressStartAtJit

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NETFramework\DisableConfigCache

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\VersioningLog

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index12a\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index12a\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\EvaluationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83>Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83>Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,x86
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\Latest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\index20
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\LegacyPolicyTimeStamp
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\30bc7c4f\3f50fe4f\88\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\30bc7c4f\3f50fe4f\88\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\30bc7c4f\3f50fe4f\88\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\30bc7c4f\3f50fe4f\88\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\30bc7c4f\3f50fe4f\88\EvaluationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\30bc7c4f\3f50fe4f\88>Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\30bc7c4f\3f50fe4f\88\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\30bc7c4f\3f50fe4f\88\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\30bc7c4f\3f50fe4f\88\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\424bd4d8\1c83327b\86\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\424bd4d8\1c83327b\86>Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\424bd4d8\1c83327b\86\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\424bd4d8\1c83327b\86\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\424bd4d8\1c83327b\86\LastModTime

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\IL\19ab8d57\1bd7b0d8\87\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\IL\19ab8d57\1bd7b0d8\87>Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\IL\19ab8d57\1bd7b0d8\87\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\IL\19ab8d57\1bd7b0d8\87\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\IL\19ab8d57\1bd7b0d8\87\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\IL\3f50fe4f6f1da7aa\88\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\IL\3f50fe4f6f1da7aa\88>Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\IL\3f50fe4f6f1da7aa\88\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\IL\3f50fe4f6f1da7aa\88\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\IL\3f50fe4f6f1da7aa\88\LastModTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\System,2.0.0.0,,b77a5c561934e089,MSIL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\System.Xml,2.0.0.0,,b77a5c561934e089,MSIL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\System.Configuration,2.0.0.0,,b03f5f7f11d50a3a,MSIL
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\NI\1c22df2f4f99a7c9\2e\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\NI\1c22df2f4f99a7c9\2e\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\NI\1c22df2f4f99a7c9\2e\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\2.0.50727_32\NI\1c22df2f4f99a7c9\2e\MVID

MODIFIED FILES

C:\Users\user\Desktop\server.exe
C:\Users\user\Desktop\server.exe.tmp
\Device\Http\Communication

RESOLVED APIS

advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
advapi32.dll.RegEnumKeyExW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
kernel32.dll.OpenProcess
kernel32.dll.TerminateProcess
kernel32.dll.WriteProcessMemory
kernel32.dll.VirtualAllocEx
advapi32.dll.AdjustTokenPrivileges

user32.dll.MessageBoxTimeoutW
wintrust.dll.WinVerifyTrust
kernel32.dll.CreateProcessInternalW
kernel32.dll.FlsAlloc
kernel32.dll.FlsFree
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.CreateEventExW
kernel32.dll.CreateSemaphoreExW
kernel32.dll.SetThreadStackGuarantee
kernel32.dll.CreateThreadpoolTimer
kernel32.dll.SetThreadpoolTimer
kernel32.dll.WaitForThreadpoolTimerCallbacks
kernel32.dll.CloseThreadpoolTimer
kernel32.dll.CreateThreadpoolWait
kernel32.dll.SetThreadpoolWait
kernel32.dll.CloseThreadpoolWait
kernel32.dll.FlushProcessWriteBuffers
kernel32.dll.FreeLibraryWhenCallbackReturns
kernel32.dll.GetCurrentProcessorNumber
kernel32.dll.GetLogicalProcessorInformation
kernel32.dll.CreateSymbolicLinkW
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.CompareStringEx
kernel32.dll.GetDateFormatEx
kernel32.dll.GetLocaleInfoEx
kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName
kernel32.dll.IsValidLocaleName
kernel32.dll.LCMapStringEx
kernel32.dll.GetTickCount64
advapi32.dll.EventRegister
mscoree.dll.#142
mscoreei.dll.RegisterShimImplCallback

mscoreei.dll.OnShimDllMainCalled
mscoreei.dll._CorExeMain
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
ws2help.dll.WahReferenceContextByHandle
ntdll.dll.KiUserExceptionDispatcher
shlwapi.dll.UrlIsW
version.dll.GetFileVersionInfoSizeW
version.dll.GetFileVersionInfoW
version.dll.VerQueryValueW
kernel32.dll.InitializeCriticalSectionAndSpinCount
kernel32.dll.IsProcessorFeaturePresent
msvcrt.dll._set_error_mode
msvcrt.dll.?set_terminate@@YAP6AXXZP6AXXZ@Z
kernel32.dll.FindActCtxSectionStringW
kernel32.dll.GetSystemWindowsDirectoryW
mscoree.dll.GetProcessExecutableHeap
mscoreei.dll.GetProcessExecutableHeap
mscorwks.dll._CorExeMain
mscorwks.dll.GetCLRFunction
advapi32.dll.RegisterTraceGuidsW
advapi32.dll.UnregisterTraceGuids
advapi32.dll.GetTraceLoggerHandle
advapi32.dll.GetTraceEnableLevel
advapi32.dll.GetTraceEnableFlags
advapi32.dll.TraceEvent
mscoree.dll.IEE
mscoreei.dll.IEE
mscorwks.dll.IEE
mscoree.dll.GetStartupFlags

DELETED FILES

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.2300.25263718

C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.2300.25263718

C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2300.25263718

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\v4.0
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot
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\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir
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_CURRENT_USER\Software\Microsoft\.NETFramework
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\UseLegacyV2RuntimeActivationPolicyDefaultValue
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\OnlyUseLatestCLR
Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\Standards\v2.0.50727
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks
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\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStart
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\GCStressStartAtJit
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Policy\AppPatch
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\Policy\AppPatch\v4.0.30319.00000\mscorwks.dll
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\96ee36b80ad6918ccd1e5568ab9522c27cdec7.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\CacheLocation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DownloadCacheQuotaInKB
HKEY_CURRENT_USER\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\EnableLog

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LoggingLevel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\ForceLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogFailures
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\VersioningLog
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DevOverrideEnable
HKEY_LOCAL_MACHINE\Software\Microsoft\ .NETFramework\Security\Policy\Extensions\NamedPermissionSets
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\ .NETFramework\Security\Policy\Extensions\NamedPermissionSets\Internet
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\ .NETFramework\Security\Policy\Extensions\NamedPermissionSets\LocalIntranet
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_LOCAL_MACHINE\Software\Microsoft\ .NETFramework\v2.0.50727\Security\Policy
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\LatestIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index12a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index12a\NIUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\index12a\ILUsageMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ConfigString
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MVID
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\EvaluationData
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83>Status
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\ILDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\NIDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\181938c6\7950e2c5\83\MissingDependencies
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\DisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83>Status

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\Modules
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\SIG
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\IL\7950e2c5\183e33de\83\LastModTime
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\GACChangeNotification\Default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\GACChangeNotification\Default\mscorlib,2.0.0.0,,b77a5c561934e089,x86
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\2023e96e\60333f2e
HKEY_LOCAL_MACHINE\Software\Microsoft\StrongName
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default

EXECUTED COMMANDS

C:\Users\user\Desktop\server.exe
netsh firewall add allowedprogram "C:\Users\user\Desktop\server.exe" "server.exe" ENABLE

READ FILES

C:\Windows\System32\tzres.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorlib.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Program Files\Common Files\System\sysmrv.dll
C:\Users\user\AppData\Local\Temp\96ee36b80ad6918ccd1e5568ab9522c27cdec7.exe.config
C:\Users\user\AppData\Local\Temp\96ee36b80ad6918ccd1e5568ab9522c27cdec7.exe
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index12a.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
\Device\KsecDD
C:\Windows\System32\intl.nls
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorlib.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll

C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBasic#\08d608378aa405adc844f3cf36974b8c\Microsoft.VisualBasic.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\dbfe8642a8ed7b2b103ad28e0c96418a\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\3afcd5168c7a6cb02eab99d7fd71e102\System.Windows.Forms.ni.dll
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sorttbls.nlp
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\sortkey.nlp
C:\Users\user\Desktop\server.exe.config
C:\Users\user\Desktop\server.exe
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui
C:\Users\user\Desktop\server.exe.tmp
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\bc09ad2d49d8535371845cd7532f9271\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\461d3b6b3f43e6fbe6c897d5936e17e4\System.Xml.ni.dll
\Device\Http\Communication
C:\Windows\SysWOW64\en-US\FWCFG.DLL.mui
C:\Windows\System32\DHCPQEC.DLL
C:\Windows\System32\napipsec.dll
C:\Windows\System32\en-US\napipsec.dll.mui
C:\Windows\System32\tsgqec.dll
C:\Windows\System32\EAPQEC.DLL
C:\Windows\System32\en-US\eapqec.dll.mui
C:\Windows\SysWOW64\en-US\P2PNETSH.DLL.mui

MUTEXES

Global\CLR_CASOFF_Mutex
a559de6ef252a09ac222d15540e8f6a4
Global\.net clr networking

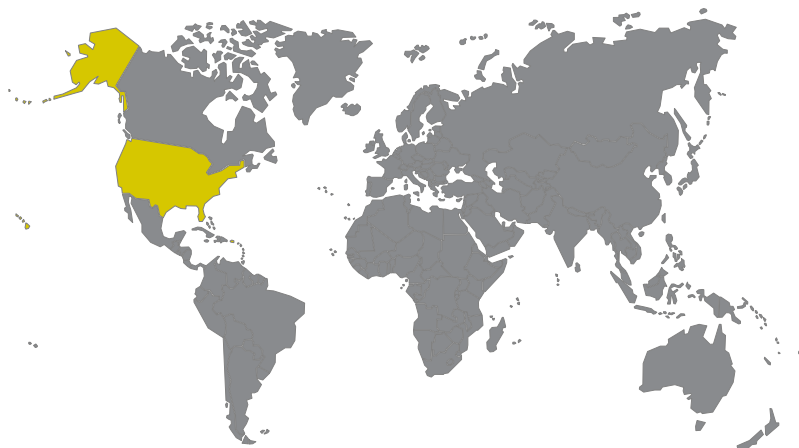
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\A559DE6EF252A09AC222D15540E8F6A4
HKEY_CURRENT_USER\Software\A559DE6EF252A09AC222D15540E8F6A4\US
HKEY_CURRENT_USER\Environment\SEE_MASK_NOZONECHECKS
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-100
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-101
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-103
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\dhcpqec.dll,-102

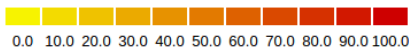
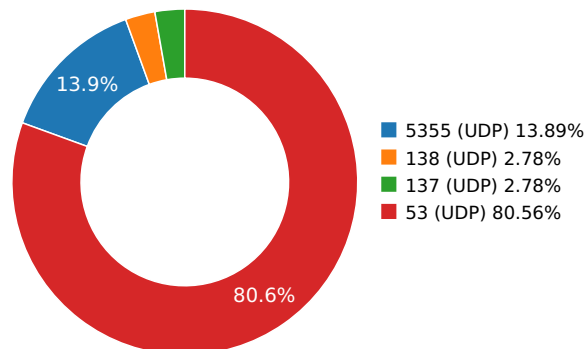
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-1
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-2
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-4
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\napipsec.dll,-3
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-100
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-101
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-102
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\tsgqec.dll,-103
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\leapqec.dll,-100
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\leapqec.dll,-101
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\leapqec.dll,-102
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\@%SystemRoot%\system32\leapqec.dll,-103

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
	45.33.2.79		63949	Akamai Technologies, Inc.	Malware Process
	23.200.3.20		20940	Akamai Technologies, Inc.	Malware Process

DNS QUERIES

Request	Type
5isohu.com	A
www.msftncsi.com	A
www.aieov.com	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
8.05742120743	Sandbox	224.0.0.252	5355
8.06435322762	Sandbox	224.0.0.252	5355
8.10590004921	Sandbox	192.168.56.255	137
8.56665611267	Sandbox	224.0.0.252	5355
10.0668342113	Sandbox	224.0.0.252	5355
10.6386470795	Sandbox	224.0.0.252	5355
11.3101220131	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
12.3094670773	Sandbox	8.8.8.8	53
12.7157552242	Sandbox	8.8.4.4	53
13.715252161	Sandbox	8.8.8.8	53
14.1525142193	Sandbox	192.168.56.255	138
25.8096690178	Sandbox	8.8.8.8	53
26.8092241287	Sandbox	8.8.4.4	53
40.1684172153	Sandbox	8.8.8.8	53
41.1682231426	Sandbox	8.8.4.4	53
54.8879380226	Sandbox	8.8.8.8	53
55.8874351978	Sandbox	8.8.4.4	53
69.2963352203	Sandbox	8.8.8.8	53
70.2936851978	Sandbox	8.8.4.4	53
83.746694088	Sandbox	8.8.8.8	53
84.7465560436	Sandbox	8.8.4.4	53
102.184576035	Sandbox	8.8.8.8	53
103.184590101	Sandbox	8.8.4.4	53
116.621898174	Sandbox	8.8.8.8	53
117.621880054	Sandbox	8.8.4.4	53
131.168648005	Sandbox	8.8.8.8	53
132.168684006	Sandbox	8.8.4.4	53
149.497160196	Sandbox	8.8.8.8	53
150.49653101	Sandbox	8.8.4.4	53
163.887642145	Sandbox	8.8.8.8	53
164.887006044	Sandbox	8.8.4.4	53
178.356396198	Sandbox	8.8.8.8	53
179.356087208	Sandbox	8.8.4.4	53
196.93494606	Sandbox	8.8.8.8	53
197.934494019	Sandbox	8.8.4.4	53
211.324886084	Sandbox	8.8.8.8	53

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\Desktop\Server.Exe	Type : PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows MD5 : 1ba88acd9206b22b8b55e903f86db7b6 SHA-1 : 96ee36b80ad6918ccd1e5568ab9522c27cdec7 SHA-256 : fad707c342f6f41c9f76434d28df10df06a52c924f SHA-512 : 8d875c4598bd603e1515cdd77083704ba376a62 Size : 73.216 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	Servidor.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	96ee36b80ad6918ccd1e5568ab9522c27cdec7
MD5:	1ba88acd9206b22b8b55e903f86db7b6
First Seen Date:	2024-11-24 15:41:49.121276 (4 days ago)
Number Of Clients Seen:	2
Last Analysis Date:	2024-11-24 15:41:49.121276 (4 days ago)
Human Expert Analysis Date:	2024-11-25 07:17:00.158457 (3 days 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	3
Trid	[[56.7, u'Generic CIL Executable (.NET, Mono, etc.)'], [21.3, u'Win64 Executable (generic)'], [10.1, u'Windows screen saver'], [5.0, u'Win32 Dynamic Link Library (generic)'], [3.4, u'Win32 Executable (generic)']]
Compilation Time Stamp	0x5AC310B9 [Tue Apr 3 05:27:21 2018 UTC]
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	1.0.0.0
InternalName	Stub.exe
FileVersion	1.0.0.0
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	Stub.exe
Entry Point	0x4101de (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	73216
Ssdeep	768:4pSOG3GqPvLzsrMHcSkVqTz43fB4O3o81rS0cG/6MGDIrT2JaazYcHeUZ:Mo3f3qskVqTzIZLndnZ6tTUanU
Sha256	fad707c342f6f41c9f76434d28df10df06a52c924fd915b09951bd2c62294f7a
Exifinfo	[[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/9/6/e/e/96ee36b80ad6918ccd1e5568ab9522c27cdec7', u'EXE:OriginalFileName': u'Stub.exe', u'EXE:InternalName': u'Stub.exe', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2024:11:24 15:41:40+00:00', u'EXE:InitializedDataSize': 14848, u'File:FileModifyDate': u'2024:11:24 15:41:19+00:00', u'EXE:AssemblyVersion': u'1.0.0.0', u'EXE:FileVersionNumber': u'1.0.0.0', u'EXE:FileVersion': u'1.0.0.0', u'File:FileSize': u'72 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'1.0.0.0', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 0, u'File:FileName': u'96ee36b80ad6918ccd1e5568ab9522c27cdec7', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'.exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2018:04:03 05:27:21+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': 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/9/6/e/e/e', u'EXE:FileDescription': u'', u'EXE:EntryPoint': u'0x4101de', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 57856, u'File:FileNodeChangeDate': u'2024:11:24 15:41:37+00:00', u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.0.0.0'}]]
Mime Type	application/x-dosexec
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0xe1e4	0xe200	5.5929722676	b0674191a97465b1ff73c929bb502c15
.rsrc	0x12000	0x3800	0x3800	3.98287079969	2989abfbf69fba60870a657d6e2e24a3
.reloc	0x16000	0xc	0x200	0.0815394123432	d0fff904de6b3ded996250744c03c5dc

PE Imports

- mscoree.dll
 - _CorExeMain

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 74848, u'sha256': u'478fe62e420007abb1a697a24cb1b80ced0a8e0a335d6ce68606efe71c4afaa2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 75144, u'sha256': u'abdc6eaa0ea69a1c506edf070a07fb12071453e08ecf3c6e35f1397d3422051f', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 76528, u'sha256': u'dc2a1f63c0882b33321345f27c07ef9f8bdb87aa687f075a474be430a1135982', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 77656, u'sha256': u'accfee1287c9f7dc25ecb19548ed246ceae1652fef5ad532914d5bb9dc9299ef', u'type': u'dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2004318071, next used block 4286019447', u'size': 744}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 78400, u'sha256': u'b76fc9f2130962dfc25029a639848894feee7e9eb1a0fe5c680e3a90671741b1', u'type': u'dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 80616, u'sha256': u'b0a40090c9bdfdd8d2f77b68d7052d1eeceb41dc5ab2eaa9c85e15104984ef1', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 84880, u'sha256': u'05507c3c1ae2629aec59c1d7c14944b8aa1492eee696d1c825c5407c929ed1e1', u'type': u'MS Windows icon resource - 6 icons, 16x16, 16 colors', u'size': 90}

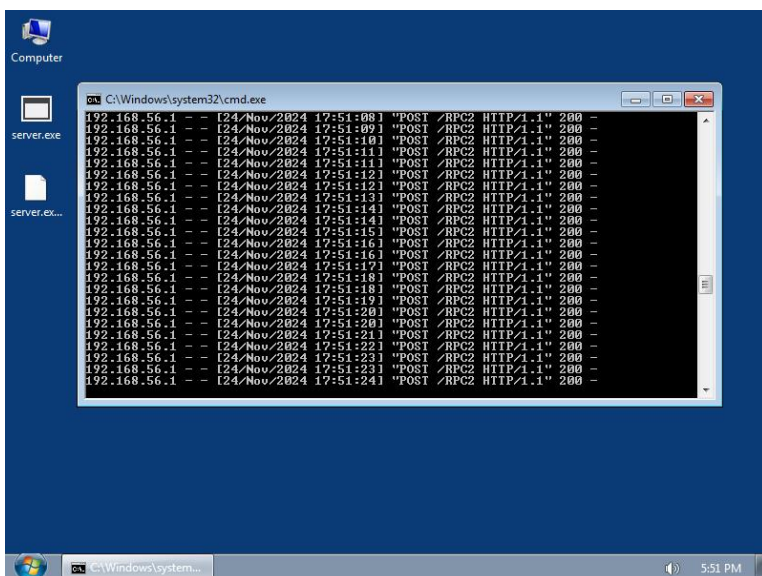
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 74272, u'sha256': u'128e7905580769c7db1c80307a394096bba9e9e7bbf40246868ee94db5b096be', u'type': u'data', u'size': 572}

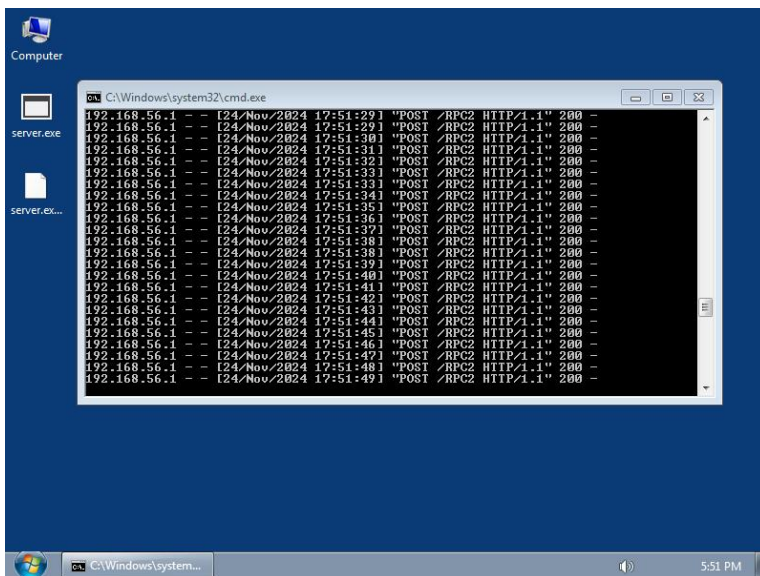
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 84976, u'sha256': u'4390603f814d79b38624fbcaffbe74eefd7a3a04b690a330a1aae7104cace3de', u'type': u'XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators', u'size': 2661}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS





```

Computer
server.exe

C:\Windows\system32\cmd.exe

Process with pid 2564
2024-11-24 17:49:12.529 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckoonon successfully loaded in process with pid 2564.
192.168.56.1 -- [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pid 2564.
2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:30] "POST /RPC2 HTTP/1.1" 200 -
  
```

```

Computer
server.exe
server.exe...

C:\Windows\system32\cmd.exe

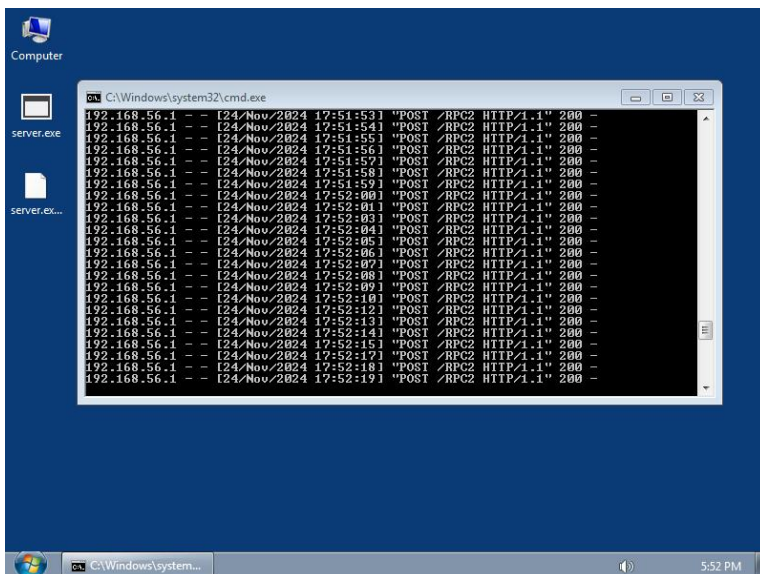
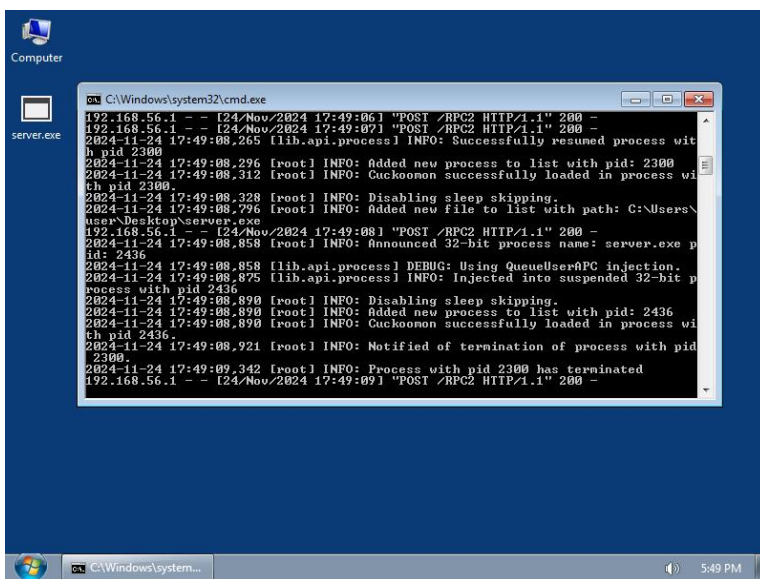
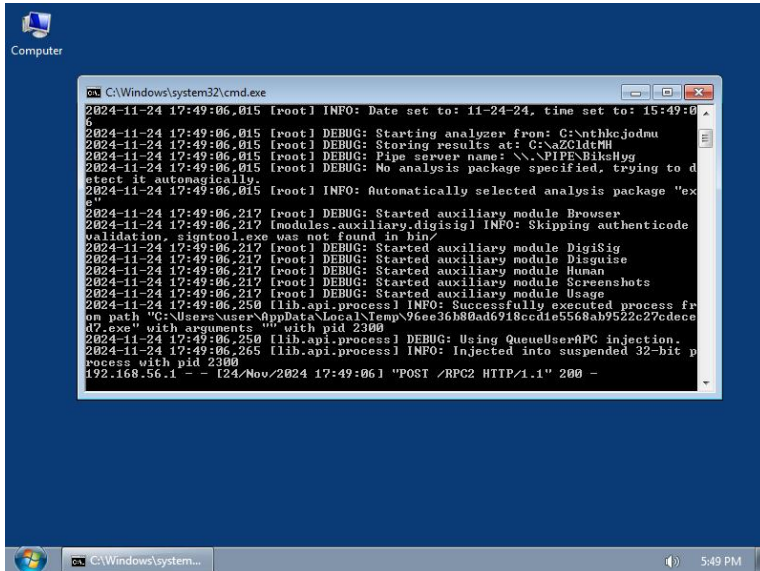
192.168.56.1 -- [24/Nov/2024 17:51:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:17] "POST /RPC2 HTTP/1.1" 200 -
  
```

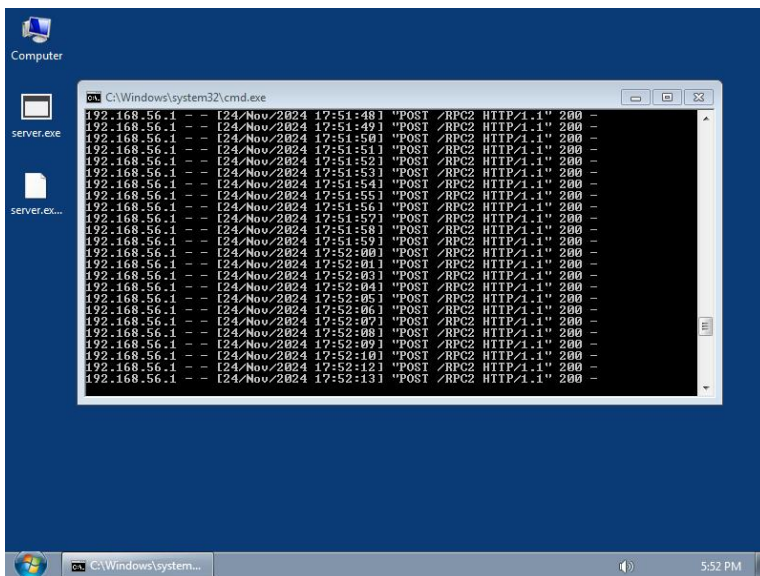
```

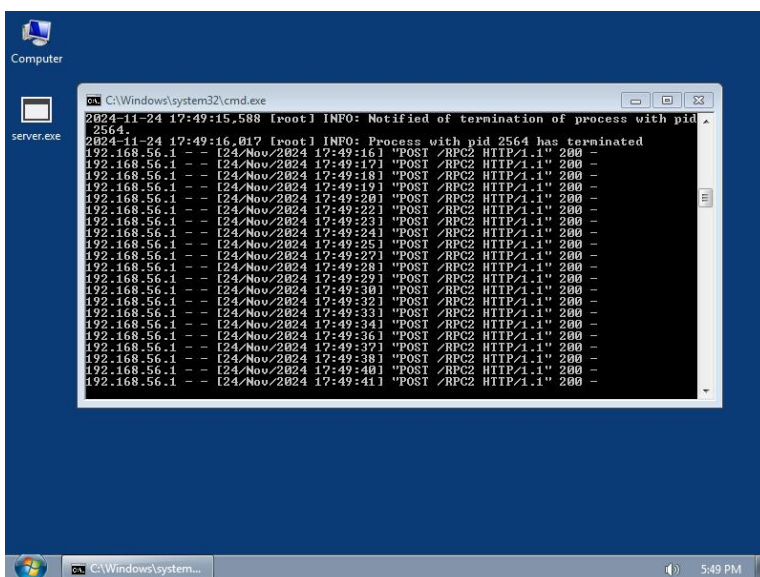
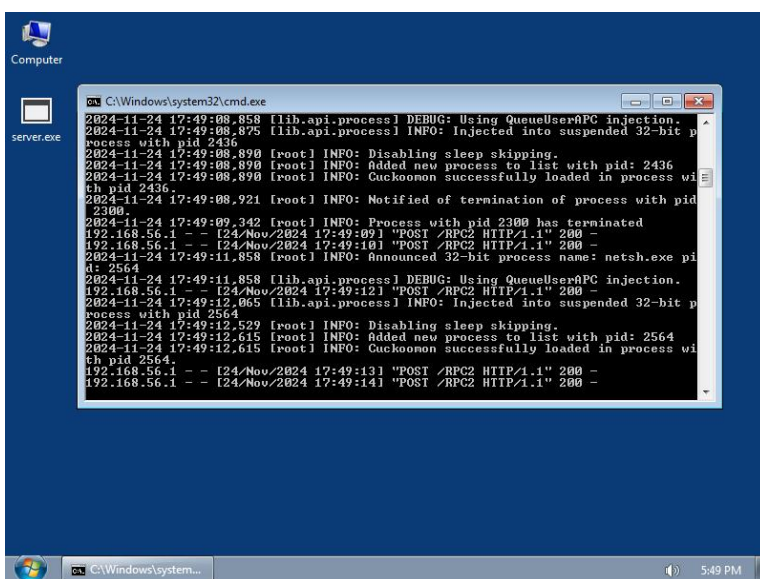
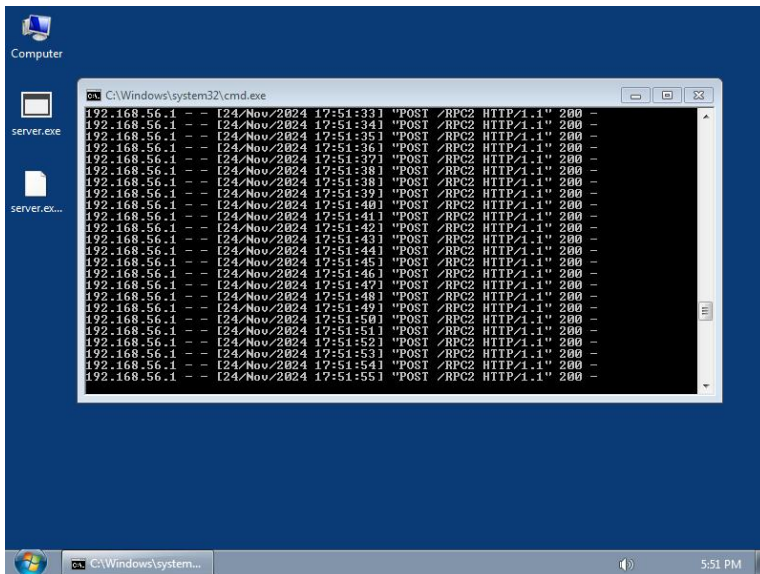
Computer
server.exe
server.exe...

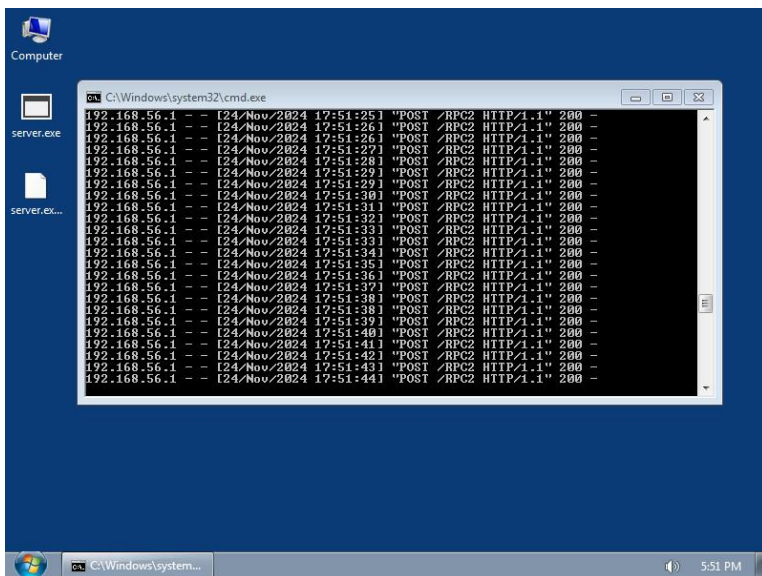
C:\Windows\system32\cmd.exe

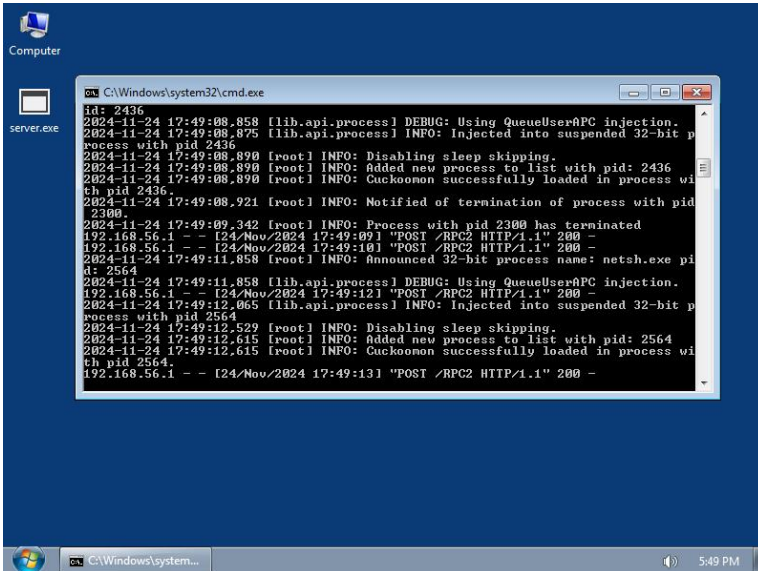
192.168.56.1 -- [24/Nov/2024 17:50:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:29] "POST /RPC2 HTTP/1.1" 200 -
  
```





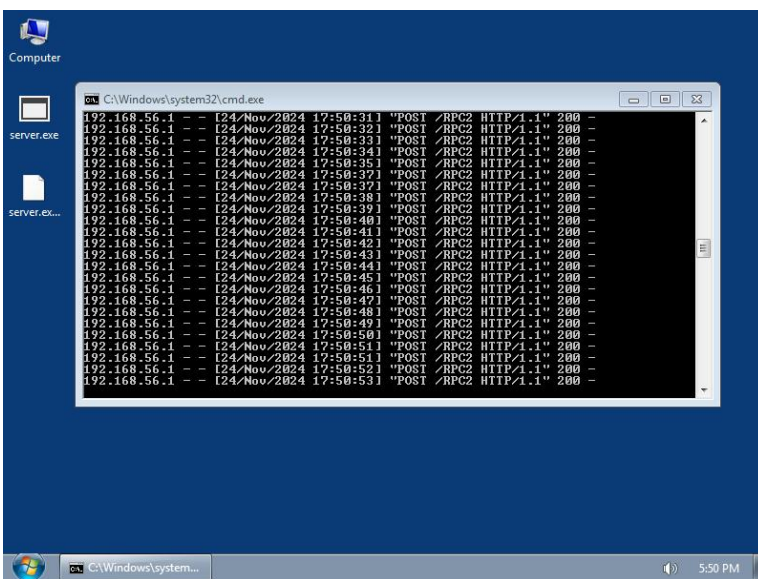






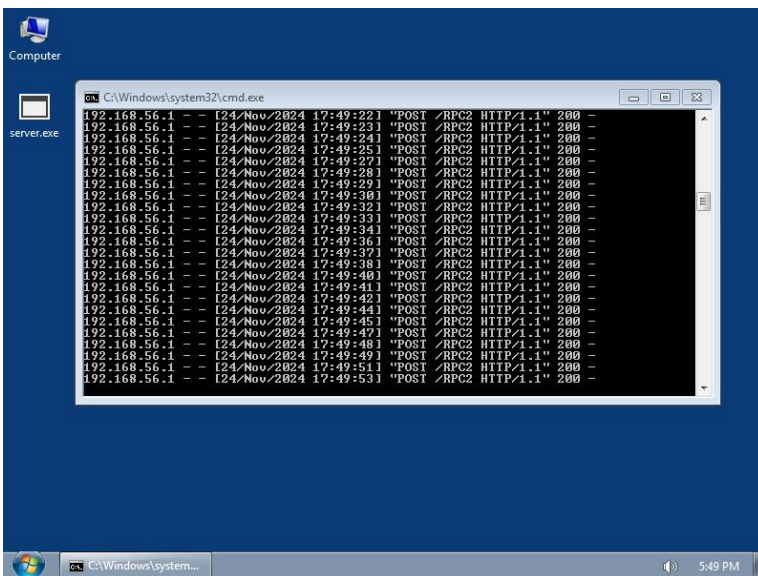
```

C:\Windows\system32\cmd.exe
11: 2436
2024-11-24 17:49:08.858 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-24 17:49:08.875 [lib.api.process] INFO: Injected into suspended 32-bit p
process with pid 2436
2024-11-24 17:49:08.890 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:08.890 [root] INFO: Added new process to list with pid: 2436
2024-11-24 17:49:08.890 [root] INFO: Cuckoonon successfully loaded in process wi
th pid 2436.
2024-11-24 17:49:08.921 [root] INFO: Notified of termination of process with pid
2300.
2024-11-24 17:49:09.342 [root] INFO: Process with pid 2300 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:10] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:11.858 [root] INFO: Announced 32-bit process name: netsh.exe pi
d 2564
2024-11-24 17:49:11.858 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 -- [24/Nov/2024 17:49:12] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:12.065 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2564
2024-11-24 17:49:12.529 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckoonon successfully loaded in process wi
th pid 2564.
192.168.56.1 -- [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
  
```



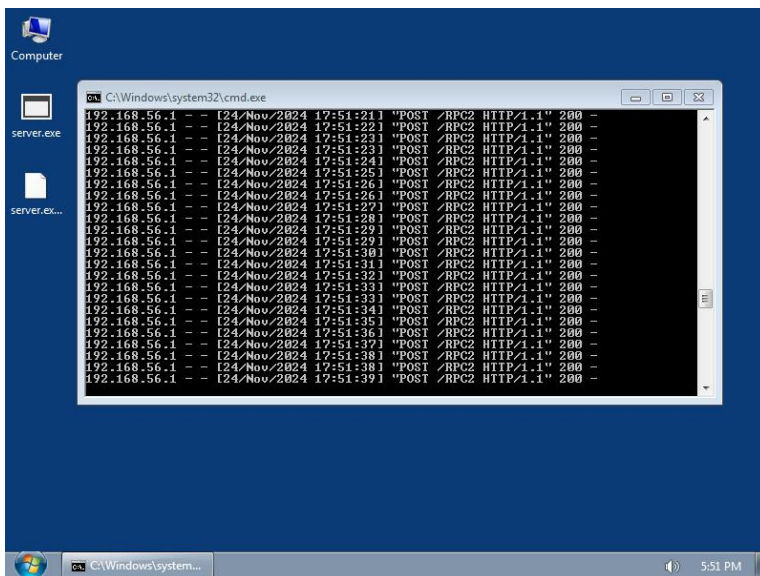
```

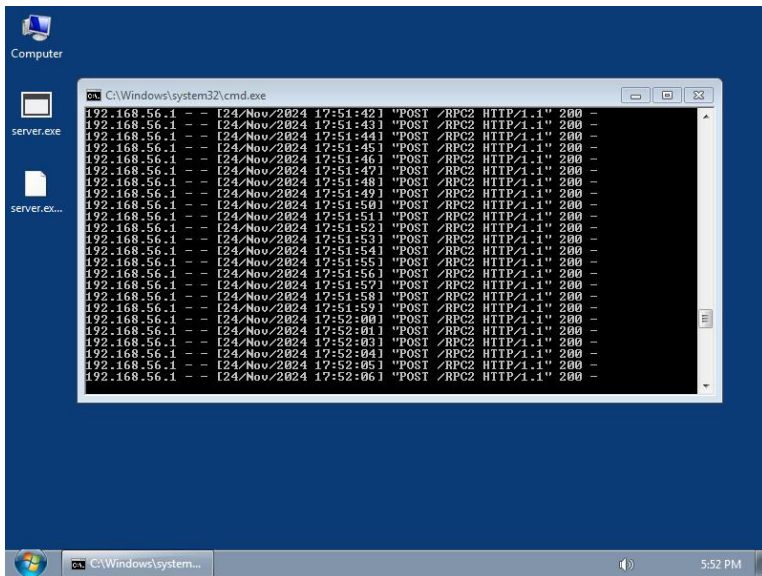
C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:50:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:53] "POST /RPC2 HTTP/1.1" 200 -
  
```



```

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:53] "POST /RPC2 HTTP/1.1" 200 -
  
```





```

Computer
server.exe

C:\Windows\system32\cmd.exe
192.168.56.1 - - [24/Nov/2024 17:49:07] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:08.265 [lib.api.process] INFO: Successfully resumed process with
h pid 2300
2024-11-24 17:49:08.296 [root] INFO: Added new process to list with pid: 2300
2024-11-24 17:49:08.312 [root] INFO: Cuckooon successfully loaded in process wi
th pid 2300.
2024-11-24 17:49:08.328 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:08.796 [root] INFO: Added new file to list with path: C:\Users\
user\Desktop\server.exe
192.168.56.1 - - [24/Nov/2024 17:49:08] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:08.858 [root] INFO: Announced 32-bit process name: server.exe p
id: 2436
2024-11-24 17:49:08.858 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-24 17:49:08.875 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2436
2024-11-24 17:49:08.890 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:08.890 [root] INFO: Added new process to list with pid: 2436
2024-11-24 17:49:08.890 [root] INFO: Cuckooon successfully loaded in process wi
th pid 2436.
2024-11-24 17:49:08.921 [root] INFO: Notified of termination of process with pid
2300.
2024-11-24 17:49:09.342 [root] INFO: Process with pid 2300 has terminated
192.168.56.1 - - [24/Nov/2024 17:49:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:10] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computer
server.exe
server.exe...

C:\Windows\system32\cmd.exe
192.168.56.1 - - [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:23] "POST /RPC2 HTTP/1.1" 200 -

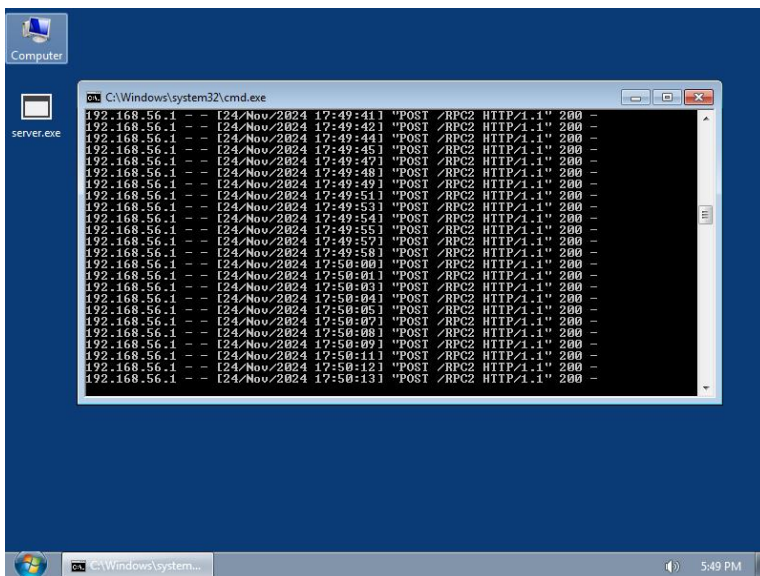
```

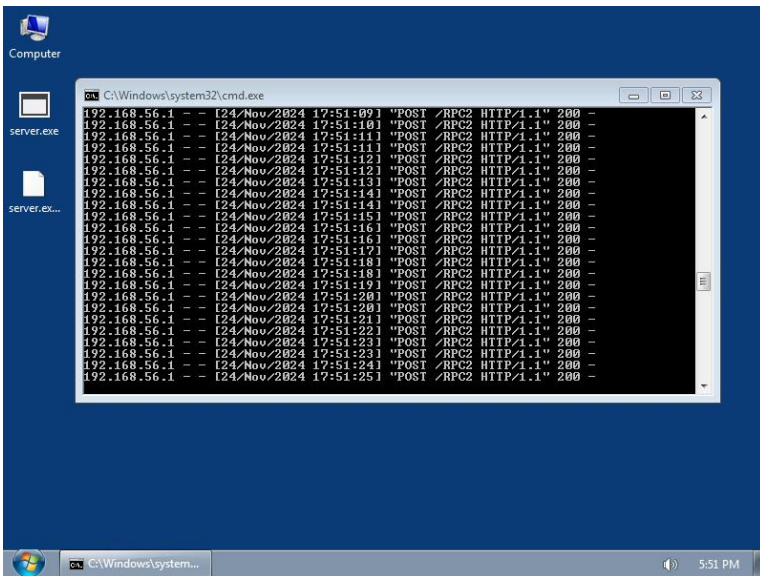
```

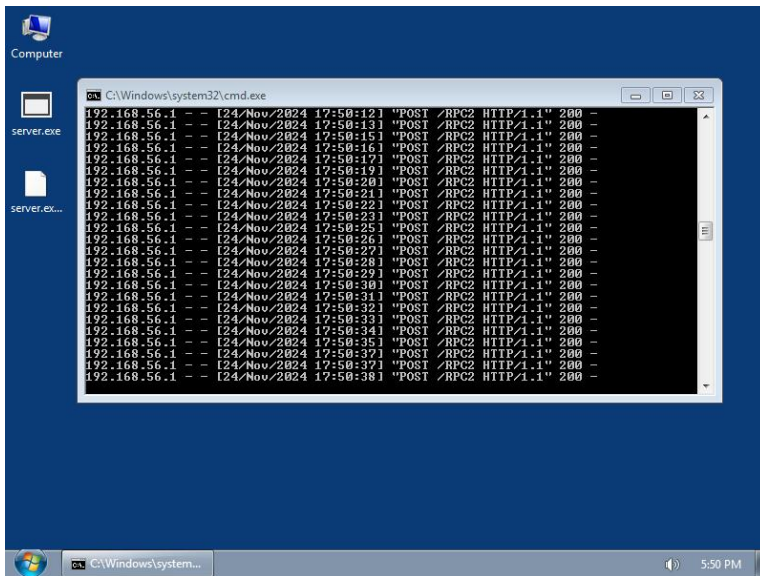
Computer
server.exe

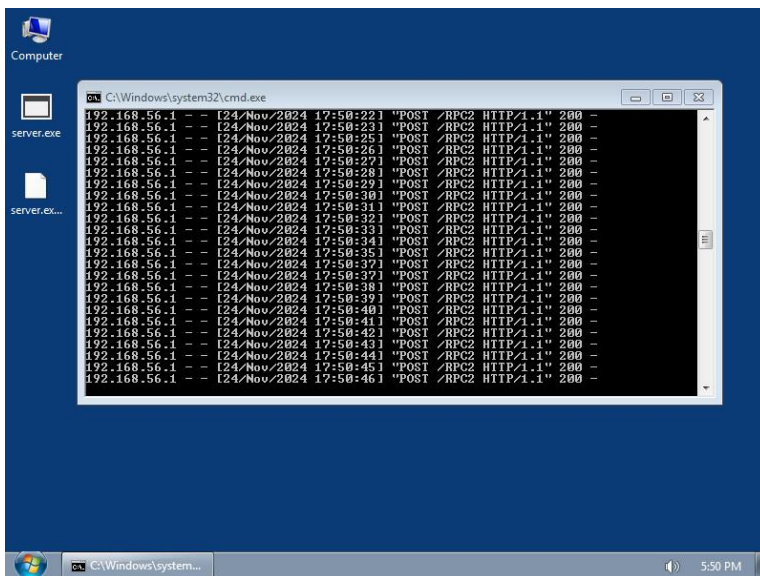
C:\Windows\system32\cmd.exe
192.168.56.1 - - [24/Nov/2024 17:49:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:16] "POST /RPC2 HTTP/1.1" 200 -

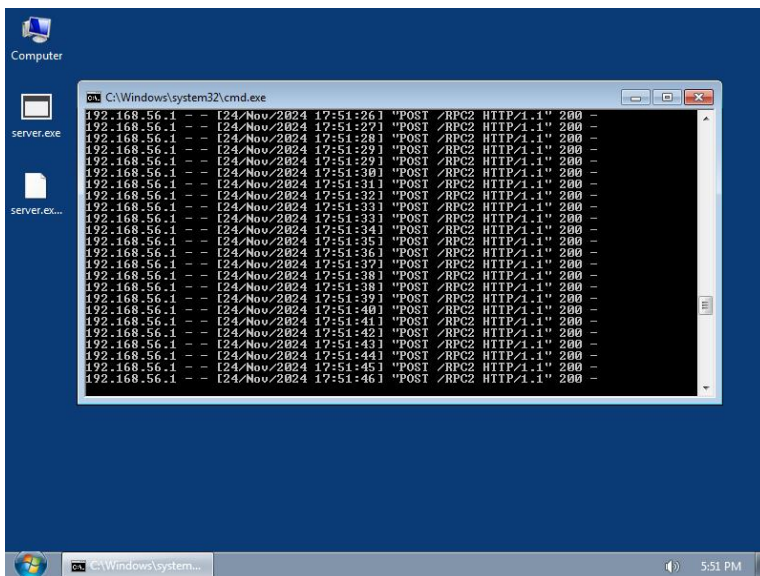
```

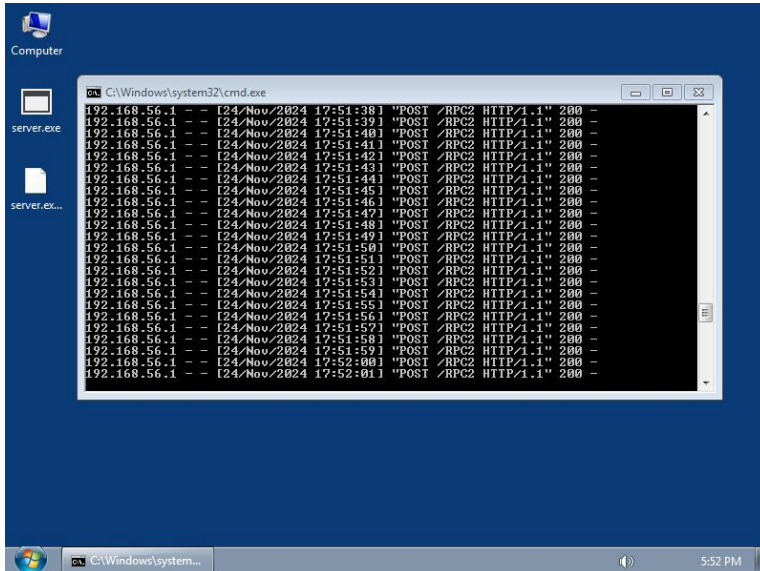







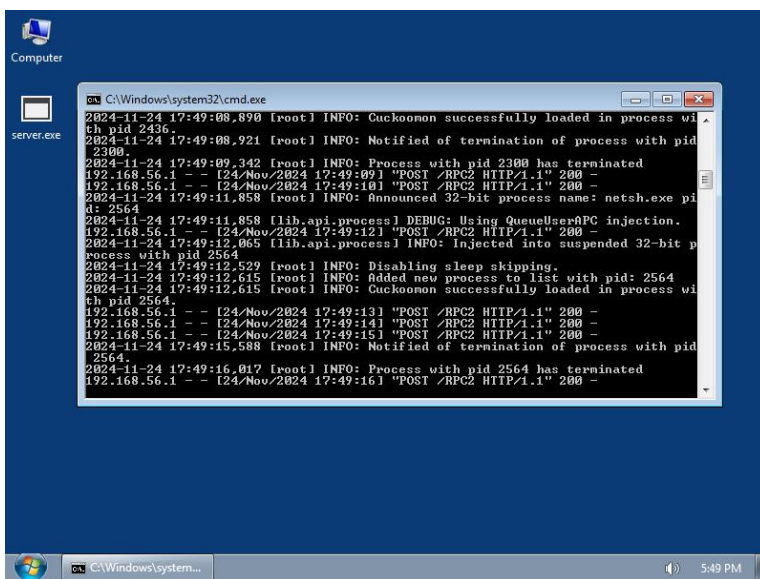






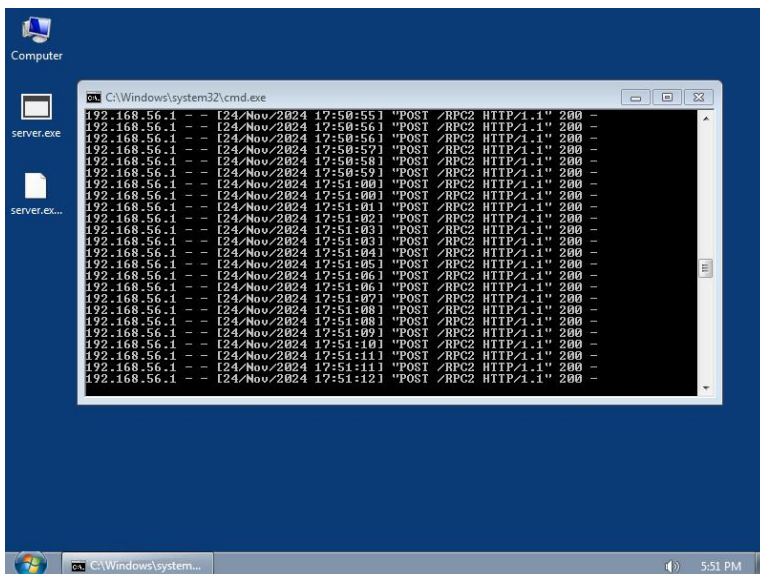
```

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:51:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:01] "POST /RPC2 HTTP/1.1" 200 -
  
```



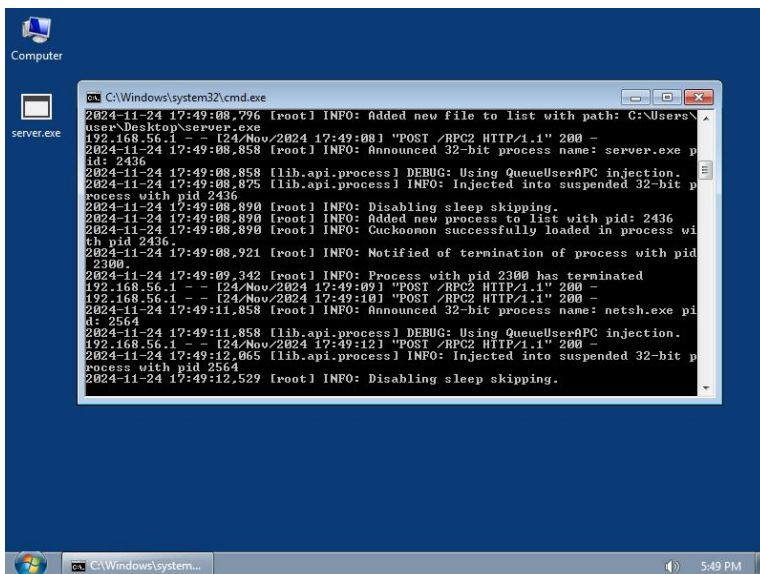
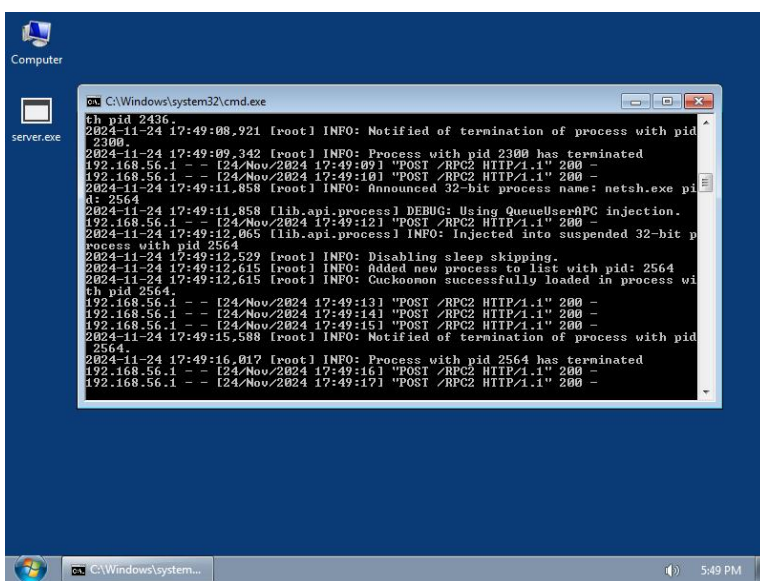
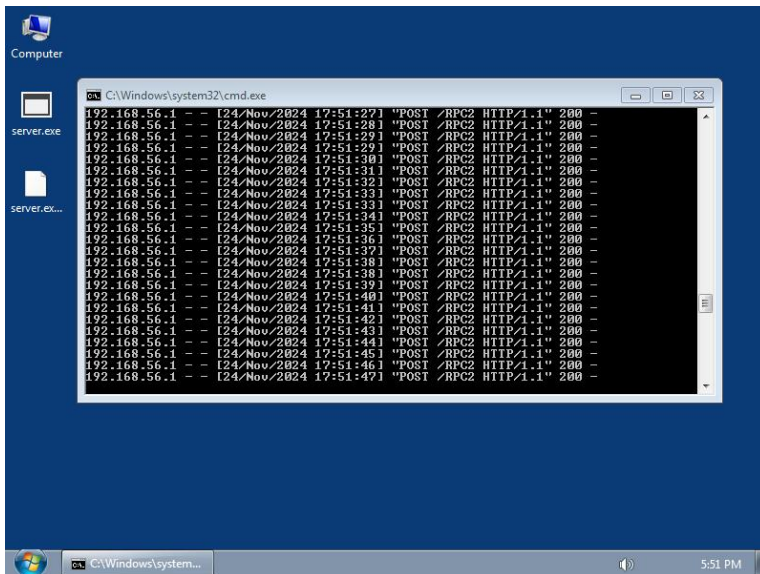
```

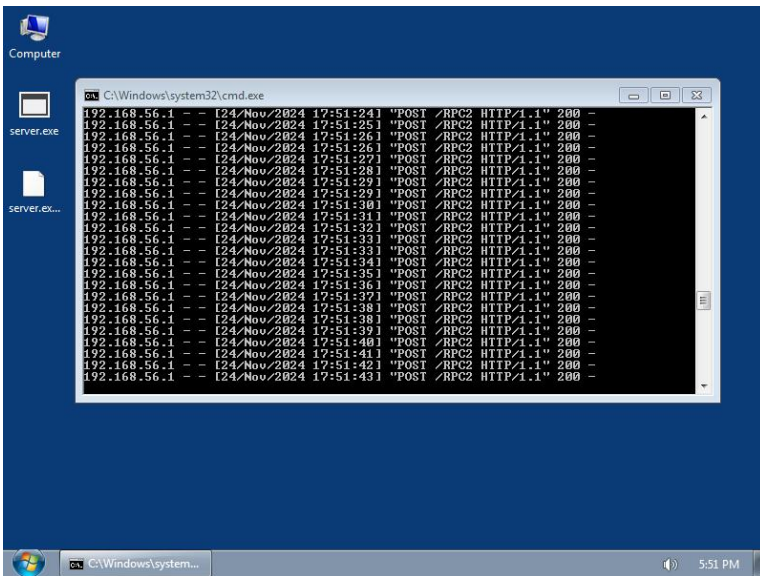
C:\Windows\system32\cmd.exe
2024-11-24 17:49:08.890 [root] INFO: Cuckoomon successfully loaded in process with pid 2436.
2024-11-24 17:49:08.921 [root] INFO: Notified of termination of process with pid 2300.
2024-11-24 17:49:09.342 [root] INFO: Process with pid 2300 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:10] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:11.858 [root] INFO: Announced 32-bit process name: netsh.exe pid: 2564
2024-11-24 17:49:11.858 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 -- [24/Nov/2024 17:49:12] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:12.065 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2564.
2024-11-24 17:49:12.529 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckoomon successfully loaded in process with pid 2564.
192.168.56.1 -- [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pid 2564.
2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
  
```

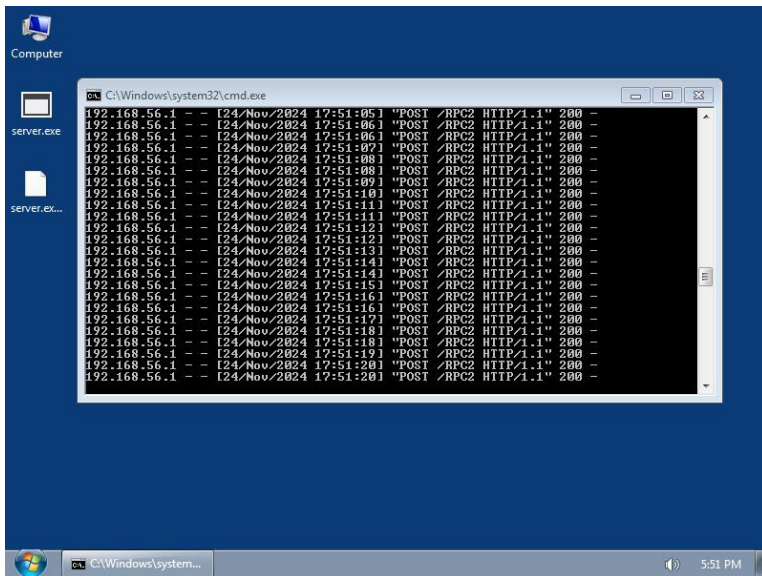


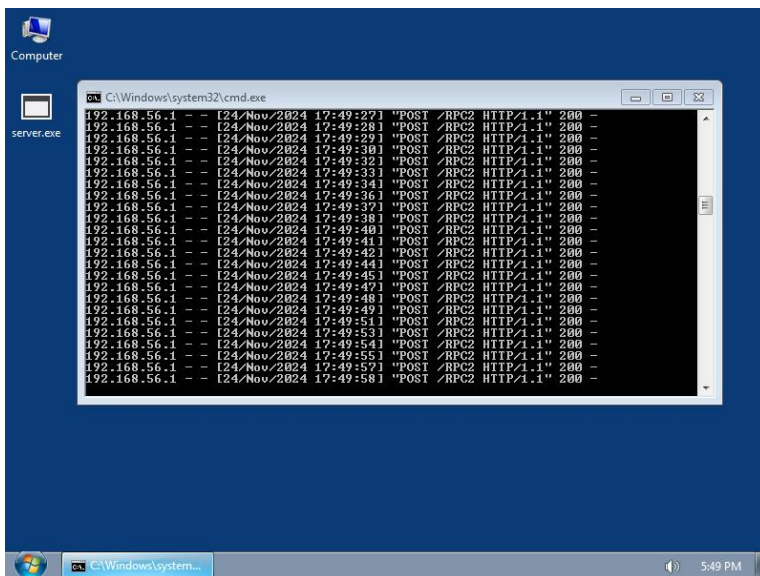
```

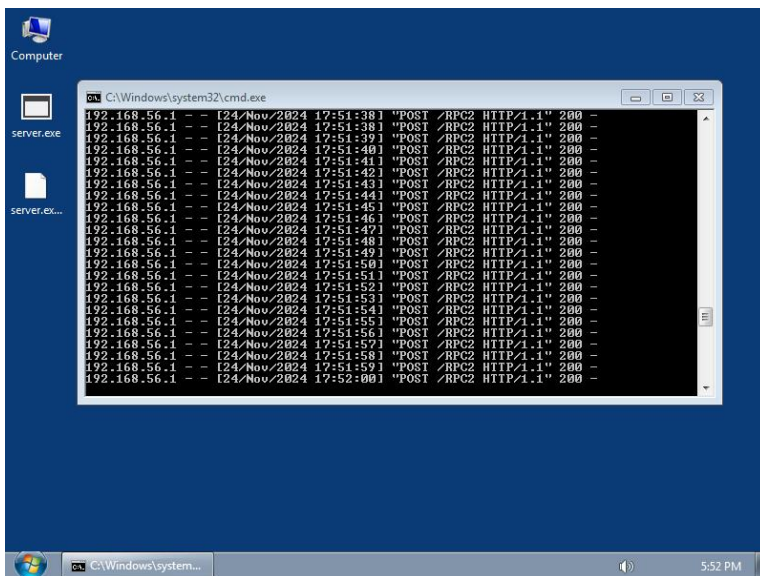
C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:50:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:12] "POST /RPC2 HTTP/1.1" 200 -
  
```

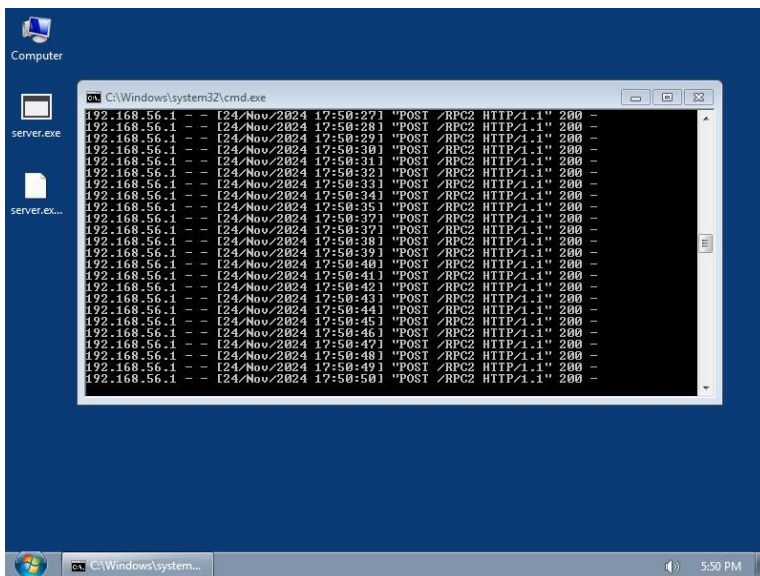


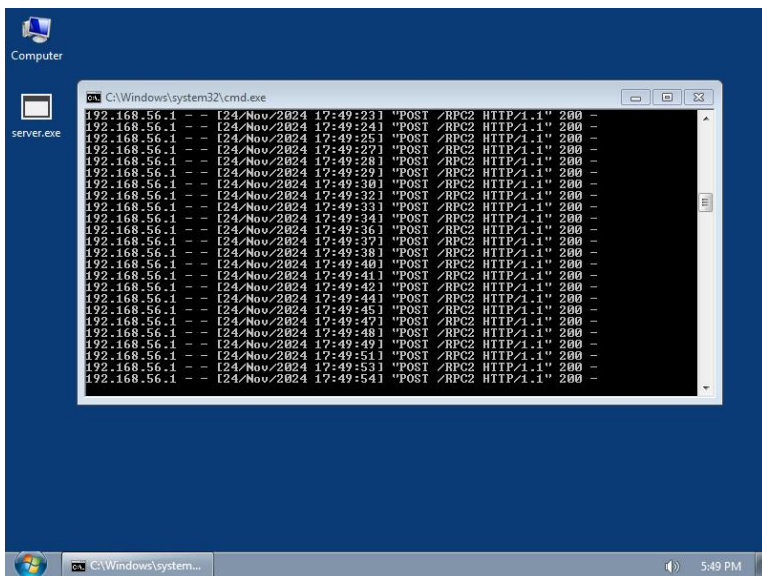


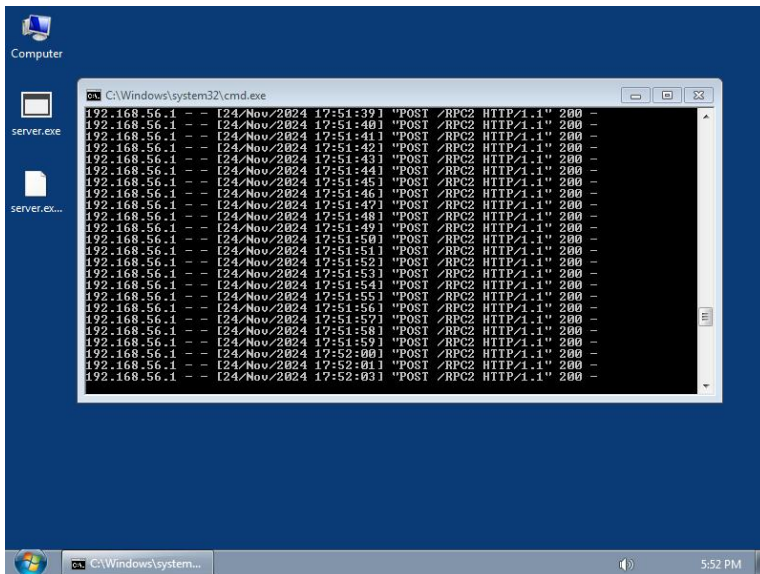













```

Computer
server.exe
server.exe...

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:50:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:00] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computer
server.exe
server.exe...

C:\Windows\system32\cmd.exe
2024-11-24 17:49:08.890 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:08.890 [root] INFO: Added new process to list with pid: 2436
2024-11-24 17:49:08.890 [root] INFO: Cuckooon successfully loaded in process with pid 2436.
2024-11-24 17:49:08.921 [root] INFO: Notified of termination of process with pid 2300.
2024-11-24 17:49:09.342 [root] INFO: Process with pid 2300 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:10] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:11.858 [root] INFO: Announced 32-bit process name: netsh.exe pid: 2564
2024-11-24 17:49:11.858 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 -- [24/Nov/2024 17:49:12] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:12.065 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2564
2024-11-24 17:49:12.529 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckooon successfully loaded in process with pid 2564.
192.168.56.1 -- [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pid 2564.

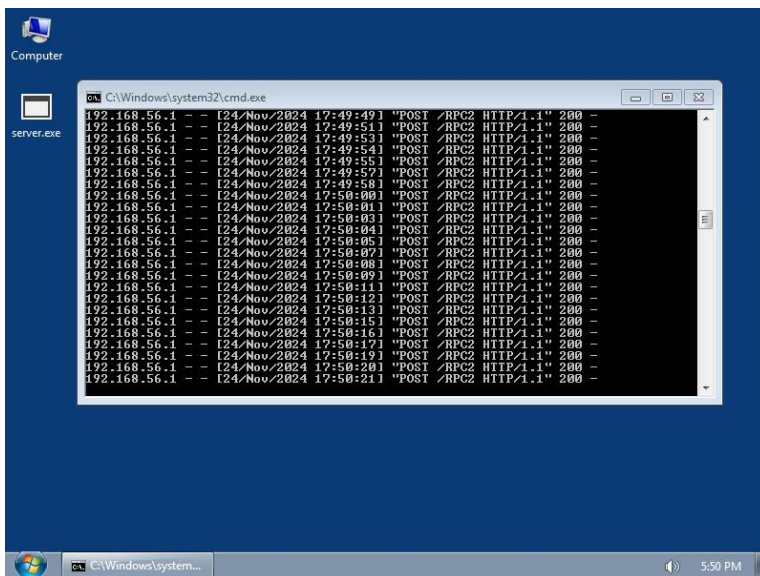
```

```

Computer
server.exe
server.exe...

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:51:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:18] "POST /RPC2 HTTP/1.1" 200 -

```



```

Computer
server.exe

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:49:10] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:11.858 [root] INFO: Announced 32-bit process name: netsh.exe pid: 2564
2024-11-24 17:49:11.858 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 -- [24/Nov/2024 17:49:12] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:12.065 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2564
2024-11-24 17:49:12.529 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckooon successfully loaded in process with pid 2564.
192.168.56.1 -- [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pid 2564.
2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computer
server.exe

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pid 2564.
2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:40] "POST /RPC2 HTTP/1.1" 200 -

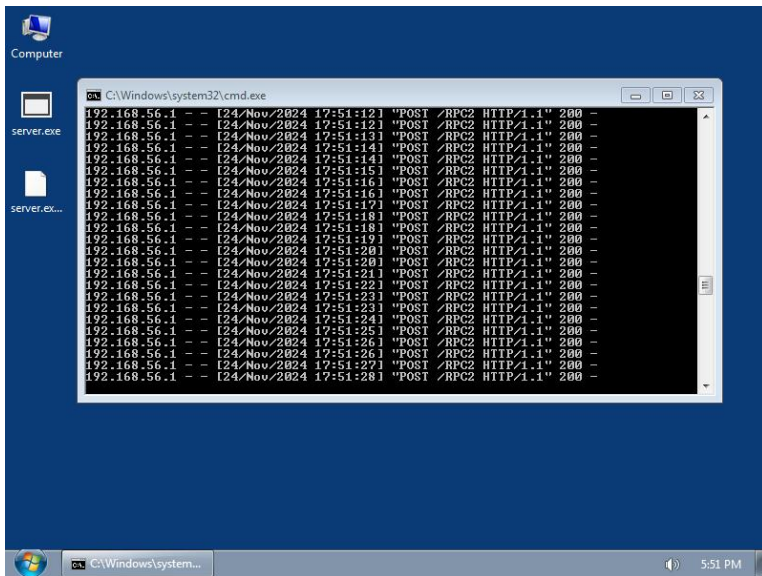
```

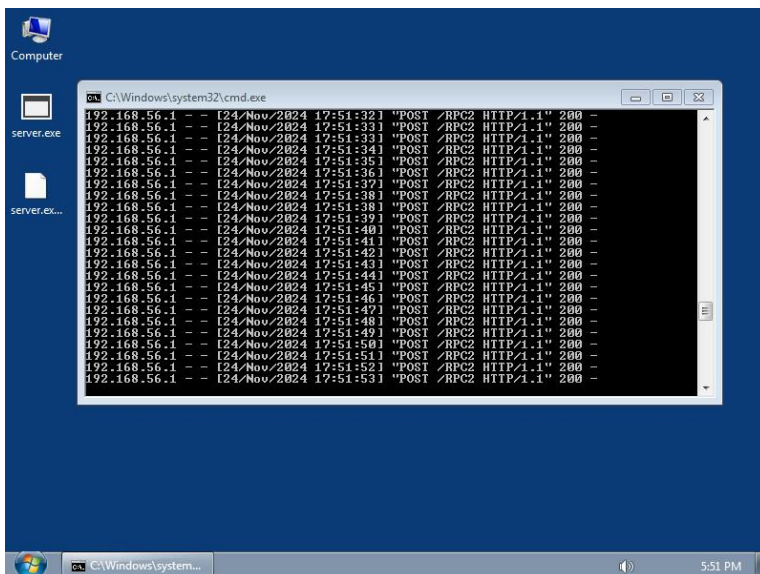
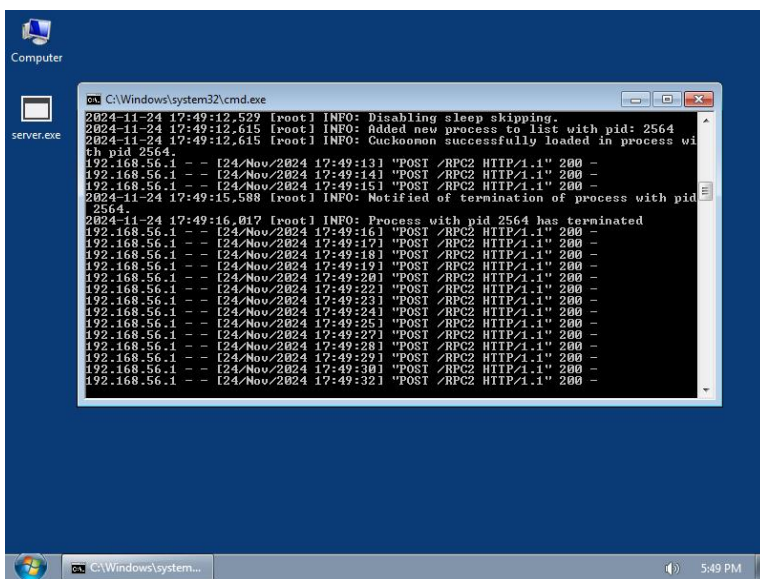
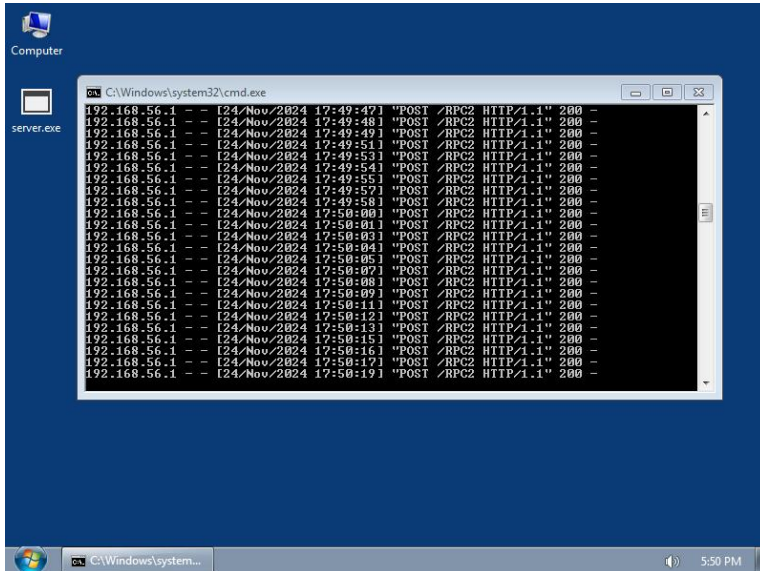
```

Computer
server.exe
server.exe...

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:51:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:45] "POST /RPC2 HTTP/1.1" 200 -

```






```

Computer
server.exe

C:\Windows\system32\cmd.exe
j: 2564
2024-11-24 17:49:11.858 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 -- [24/Nov/2024 17:49:12] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:12.065 [lib.api.process] INFO: Injected into suspended 32-bit p
process with pid 2564.
2024-11-24 17:49:12.529 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckoonon successfully loaded in process wi
th pid 2564.
192.168.56.1 -- [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pid
2564.
2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computer
server.exe
server.exe...

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:51:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:17] "POST /RPC2 HTTP/1.1" 200 -

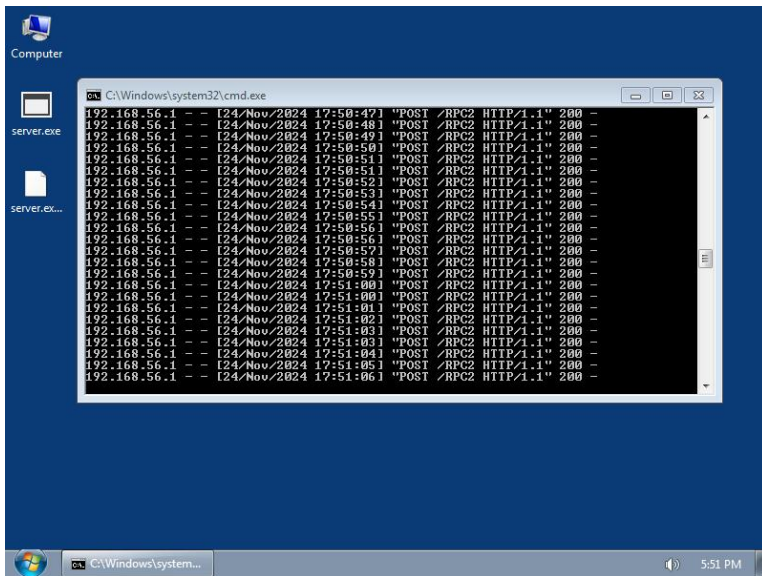
```

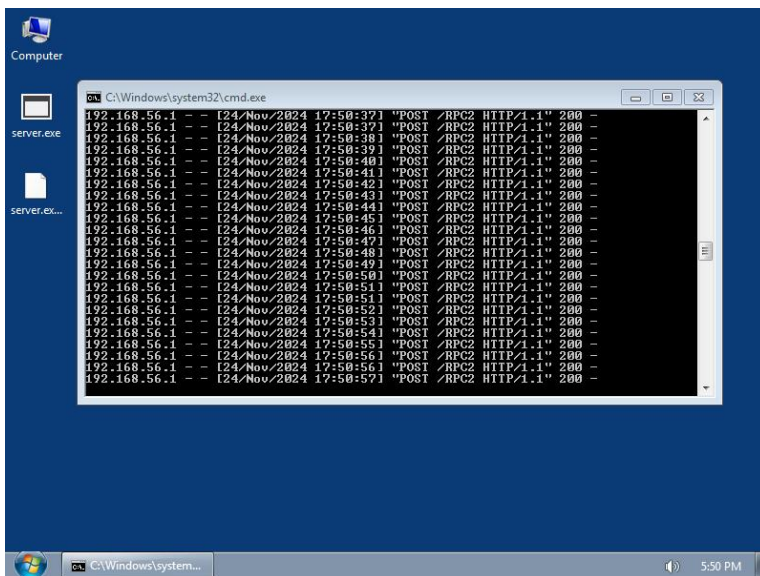
```

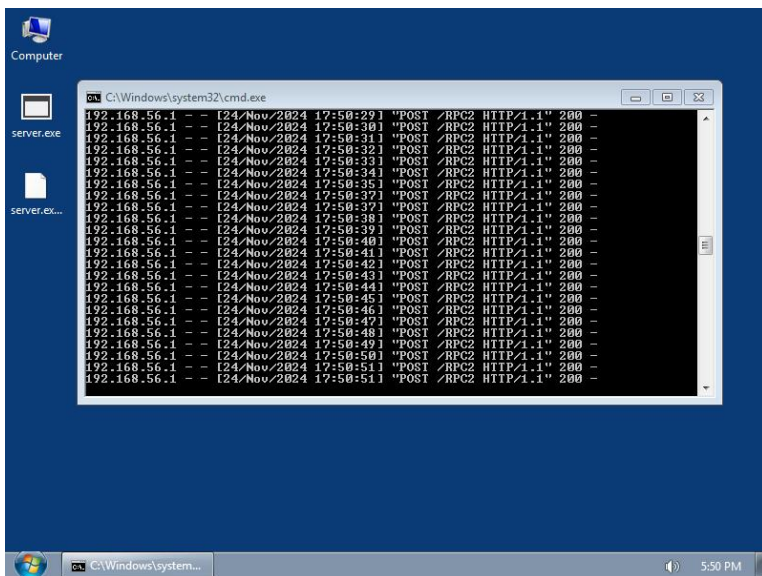
Computer
server.exe

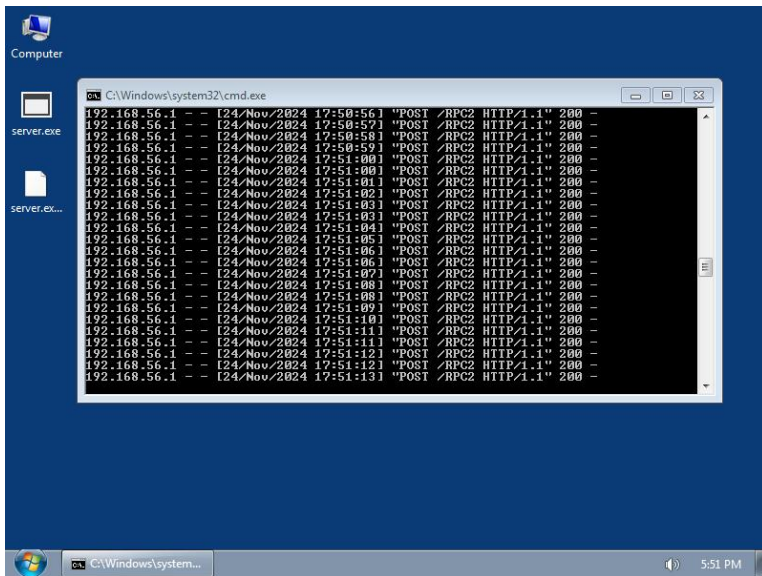
C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:48] "POST /RPC2 HTTP/1.1" 200 -

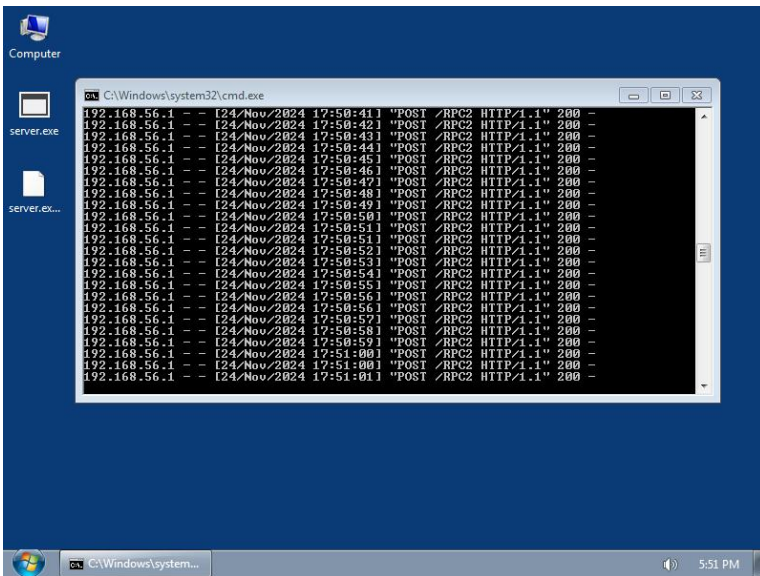
```

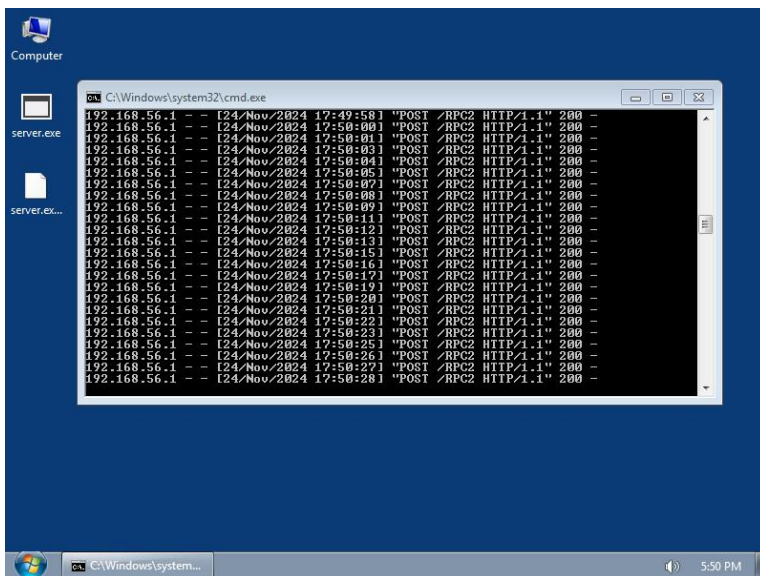


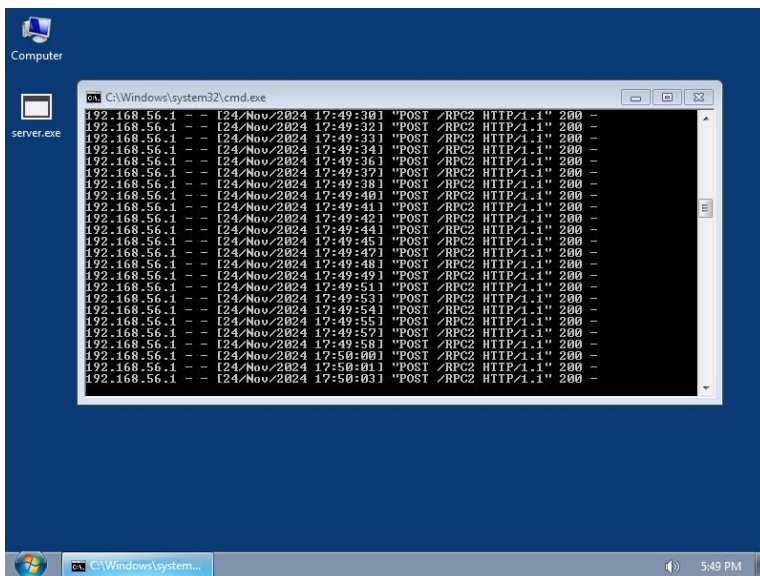


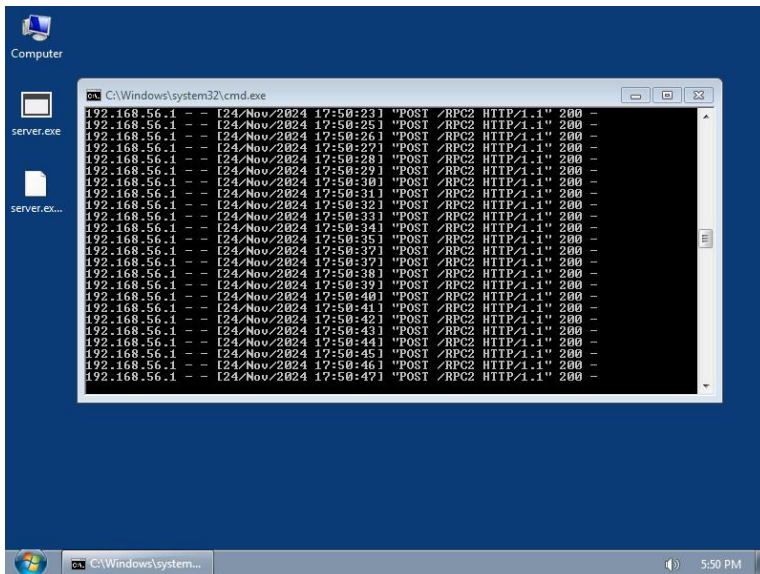








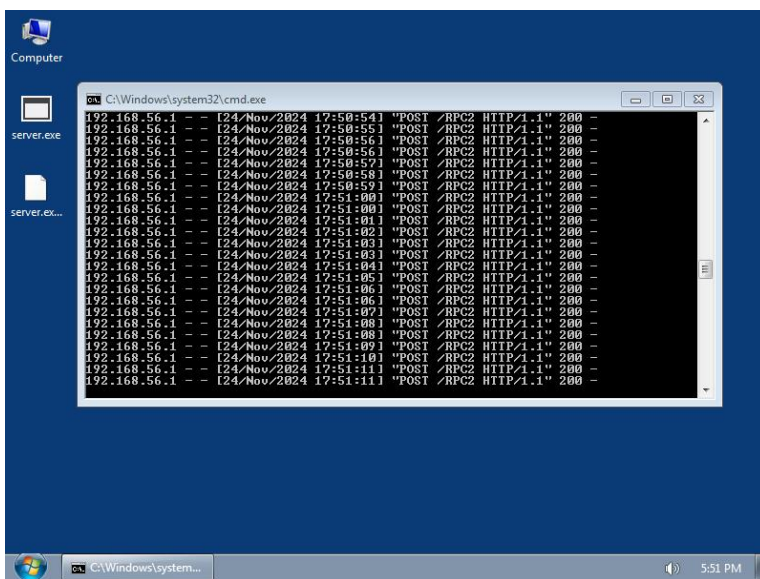




```

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:50:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:47] "POST /RPC2 HTTP/1.1" 200 -

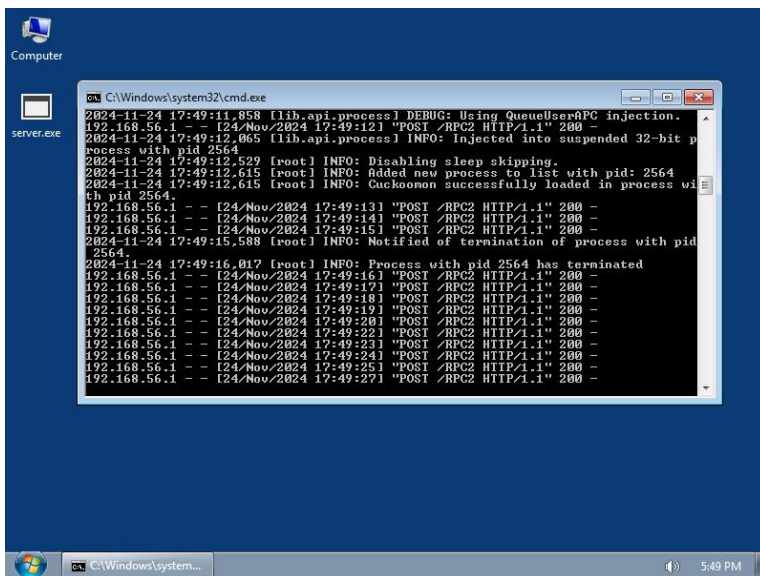
```



```

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:50:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -

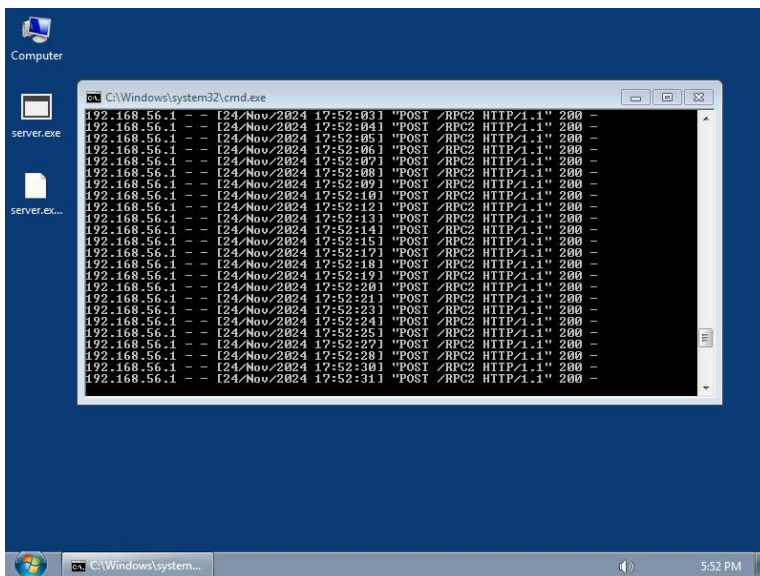
```

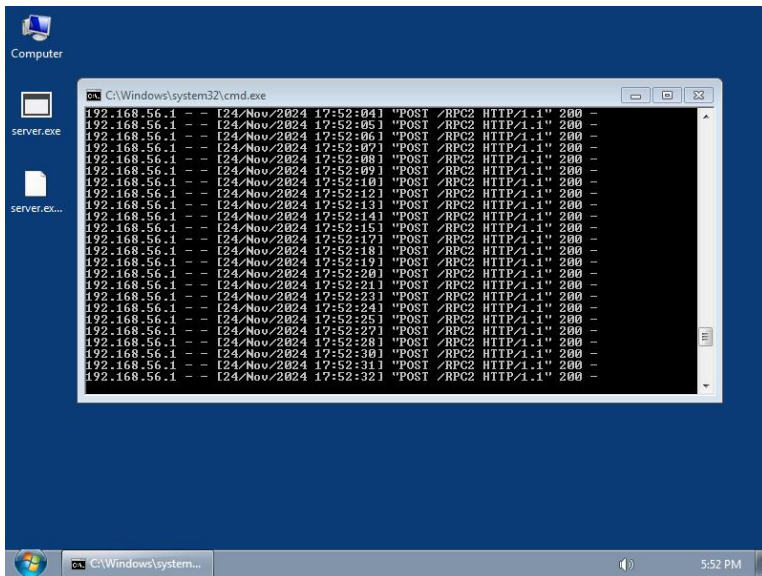


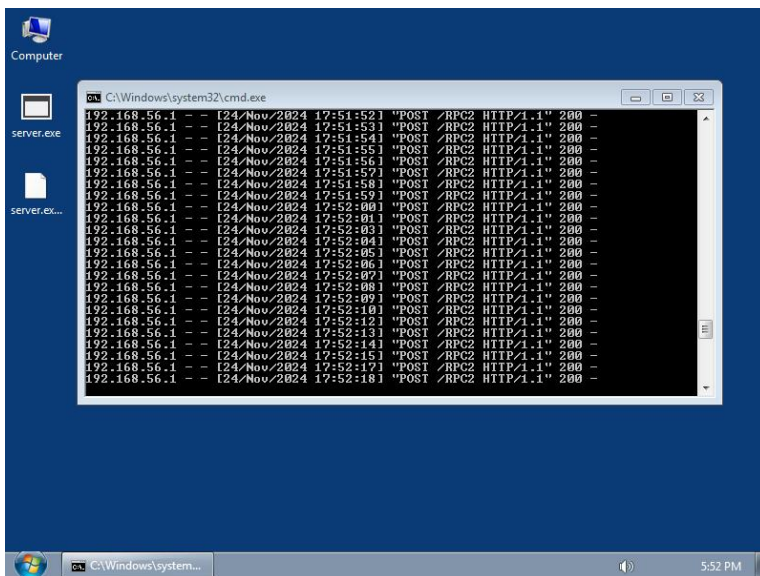
```

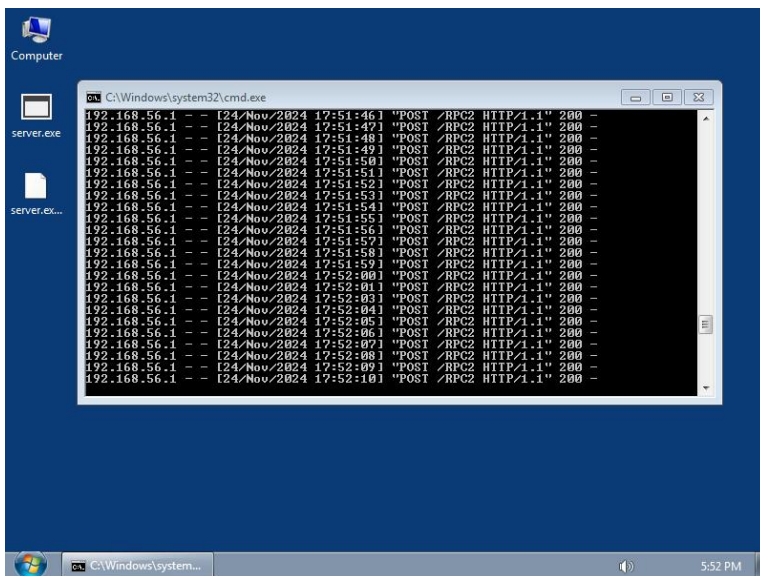
C:\Windows\system32\cmd.exe
2024-11-24 17:49:14.058 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 -- [24/Nov/2024 17:49:12] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:12.065 [lib.api.process] INFO: Injected into suspended 32-bit p
process with pid 2564.
2024-11-24 17:49:12.529 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckooemon successfully loaded in process wi
ch pid 2564.
192.168.56.1 -- [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pid
2564.
2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:27] "POST /RPC2 HTTP/1.1" 200 -

```







```

Computer
server.exe

C:\Windows\system32\cmd.exe

2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:44] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computer
server.exe
server.exe...

C:\Windows\system32\cmd.exe

192.168.56.1 -- [24/Nov/2024 17:50:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:59] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computer
server.exe

C:\Windows\system32\cmd.exe

2024-11-24 17:49:09.342 [root] INFO: Process with pid 2300 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:10] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:11.858 [root] INFO: Announced 32-bit process name: netsh.exe pi
at 2564
2024-11-24 17:49:11.858 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 -- [24/Nov/2024 17:49:12] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:12.065 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2564
2024-11-24 17:49:12.529 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckooon successfully loaded in process wi
th pid 2564.
192.168.56.1 -- [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pid
2564.
2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -

```



```

Computer
server.exe
server.exe...

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:51:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:14] "POST /RPC2 HTTP/1.1" 200 -

C:\Windows\system... 5:52 PM

```

```

Computer
server.exe
server.exe...

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:51:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:23] "POST /RPC2 HTTP/1.1" 200 -

C:\Windows\system... 5:52 PM

```

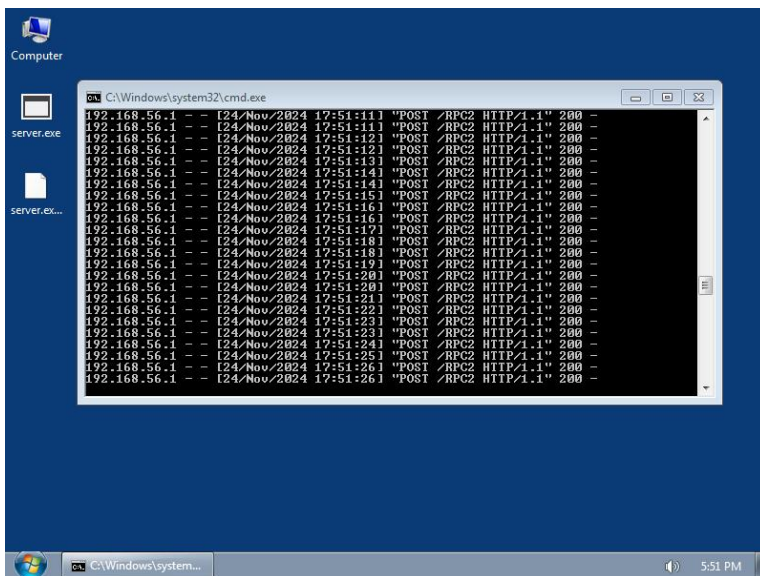
```

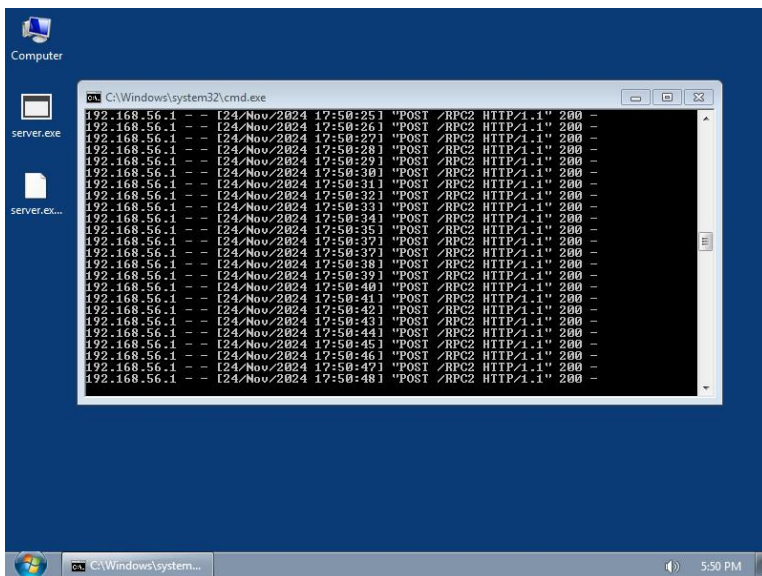
Computer
server.exe
server.exe...

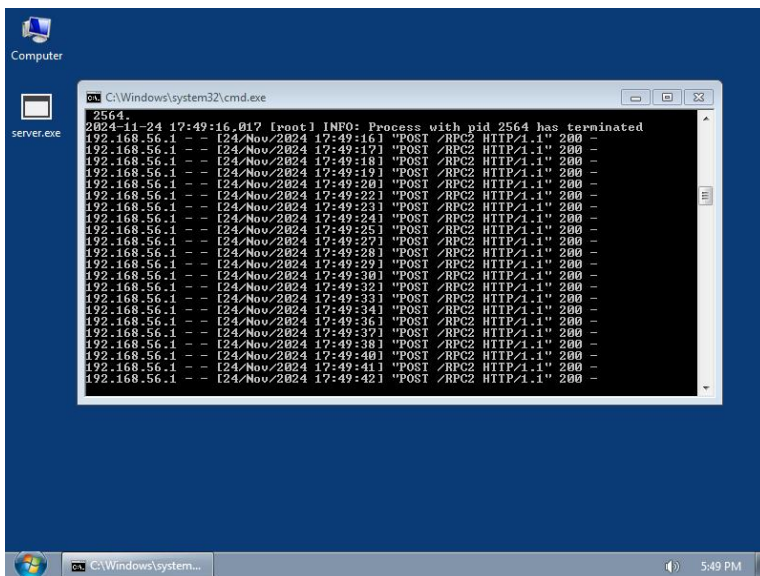
C:\Windows\system32\cmd.exe
2300
2024-11-24 17:49:09.342 [root] INFO: Process with pid 2300 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:10] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:11.858 [root] INFO: Announced 32-bit process name: netsh.exe pi
d: 2564
2024-11-24 17:49:11.858 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 -- [24/Nov/2024 17:49:12] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:12.065 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2564
2024-11-24 17:49:12.529 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckooon successfully loaded in process wi
th pid 2564.
192.168.56.1 -- [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pi
d 2564.
2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -

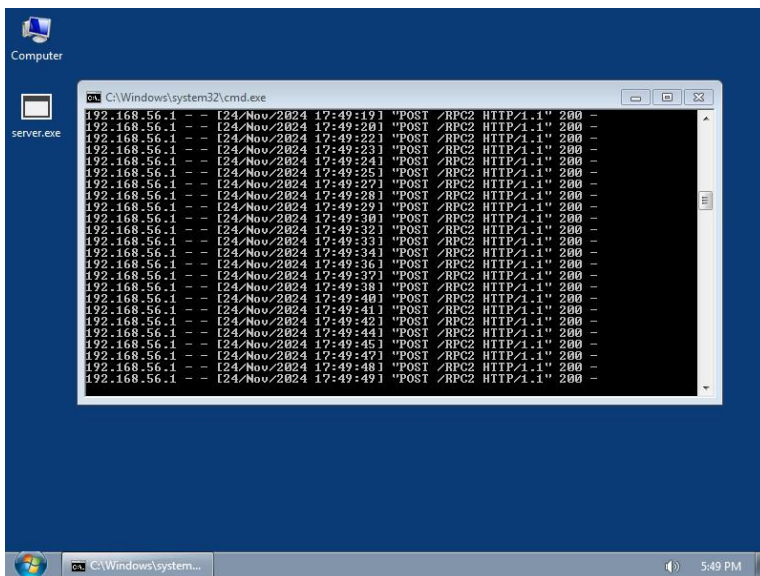
C:\Windows\system... 5:49 PM

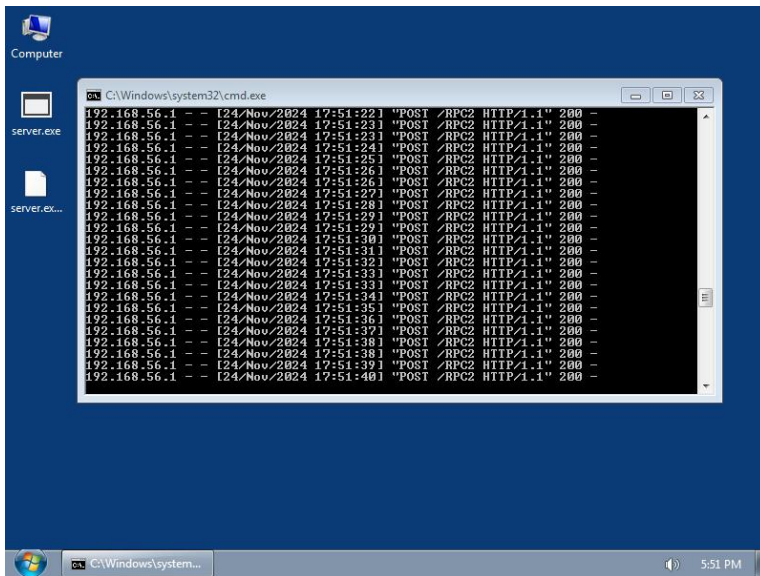
```

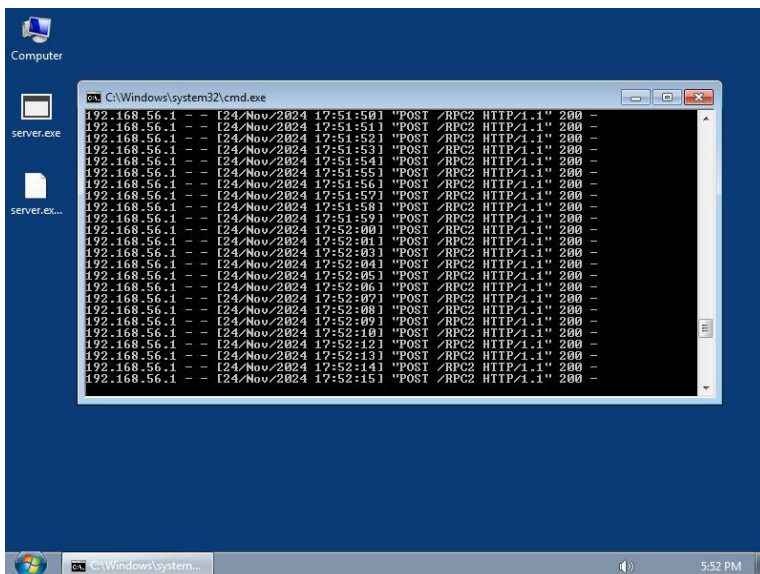
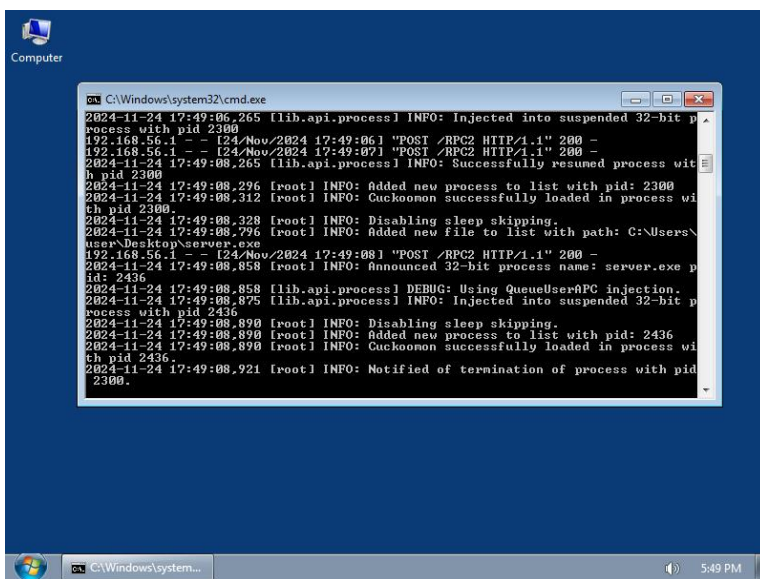
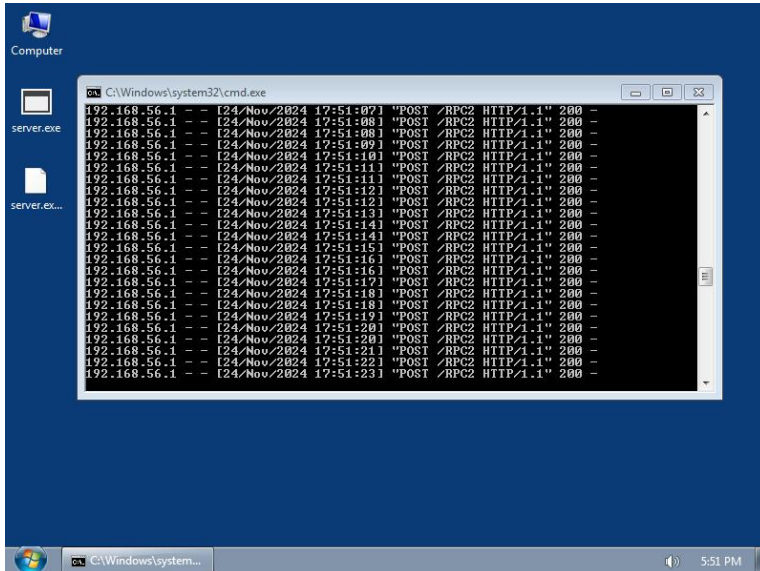



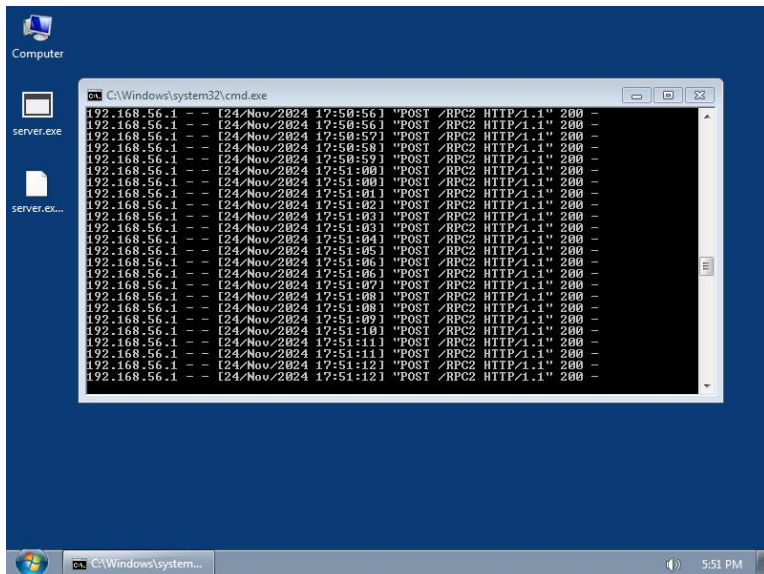








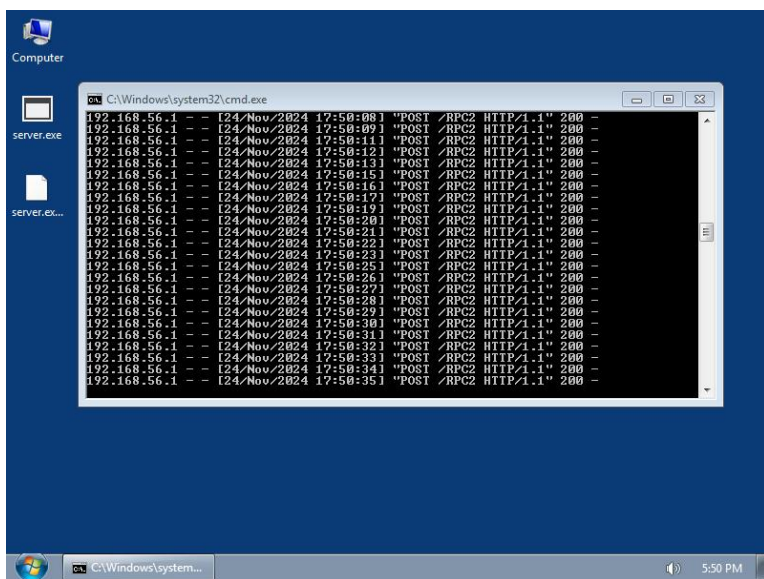




```

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:50:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:12] "POST /RPC2 HTTP/1.1" 200 -

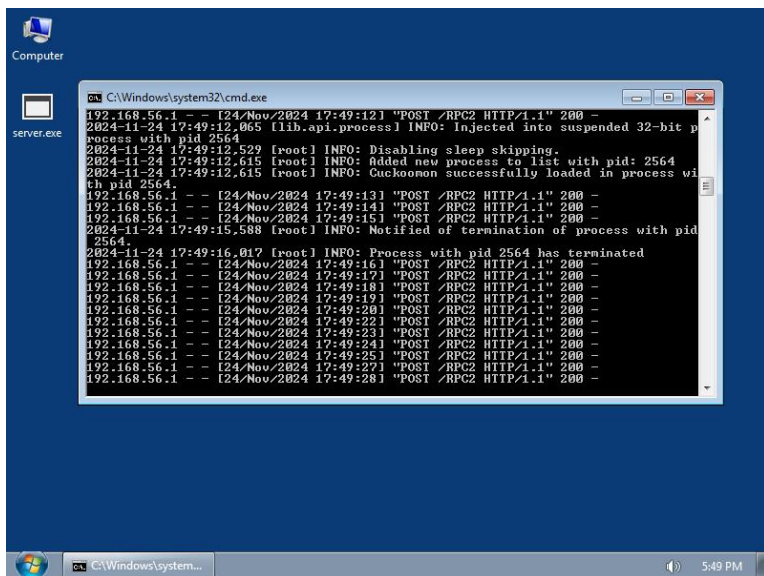
```



```

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:50:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:50:35] "POST /RPC2 HTTP/1.1" 200 -

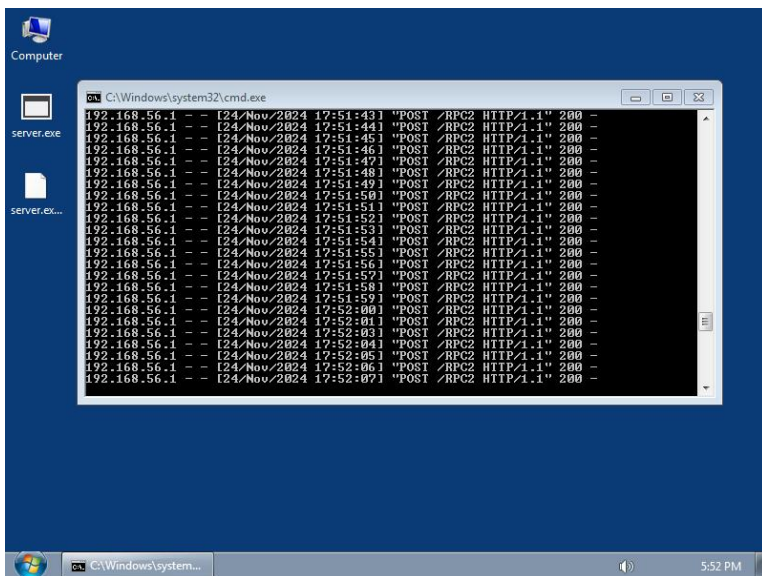
```

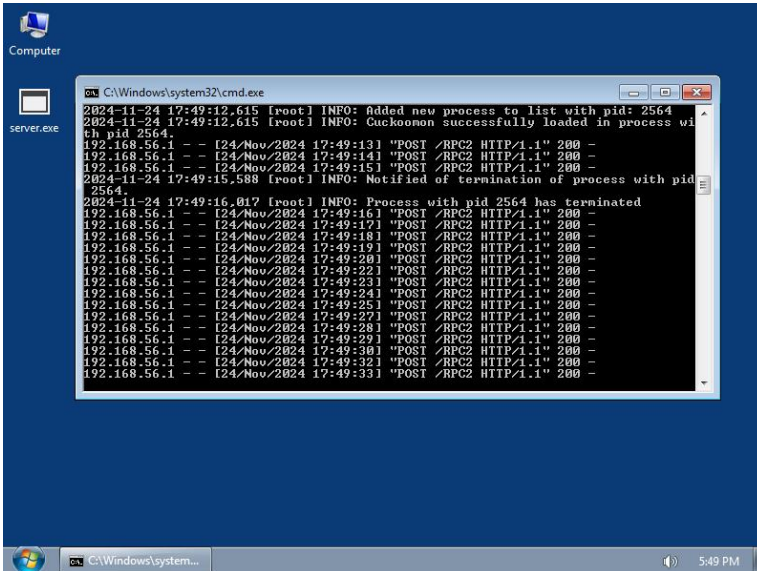


```

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:49:12] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:12.065 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2564
2024-11-24 17:49:12.529 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckooon successfully loaded in process wi
th pid 2564.
192.168.56.1 -- [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pid
2564
2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 -- [24/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:49:28] "POST /RPC2 HTTP/1.1" 200 -

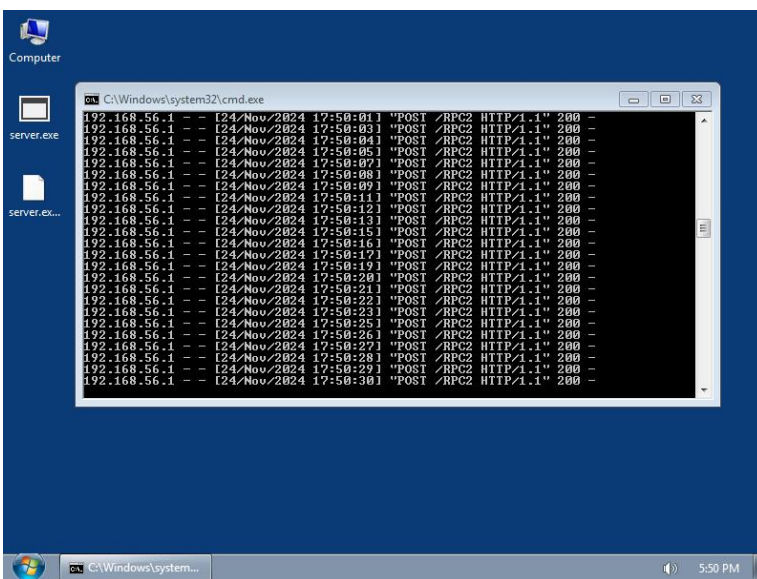
```





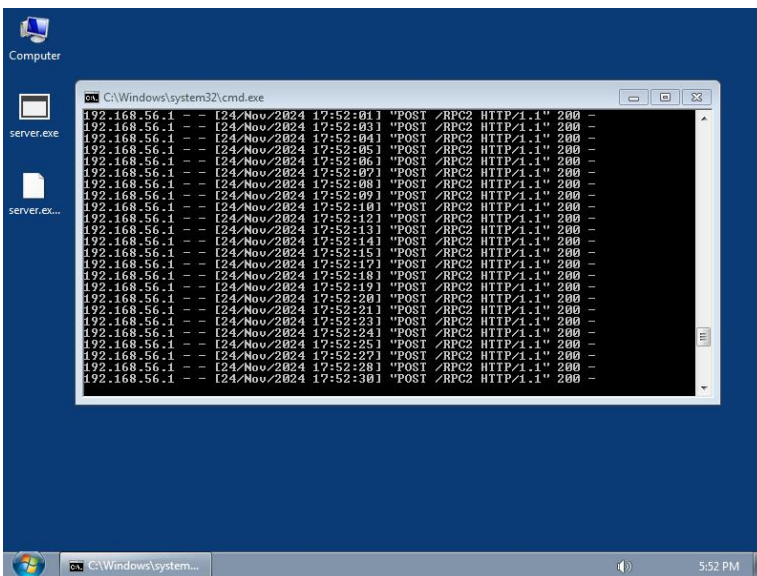
```

C:\Windows\system32\cmd.exe
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckoooon successfully loaded in process wi
th pid 2564.
192.168.56.1 - - [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pid
2564.
2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 - - [24/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:33] "POST /RPC2 HTTP/1.1" 200 -
  
```



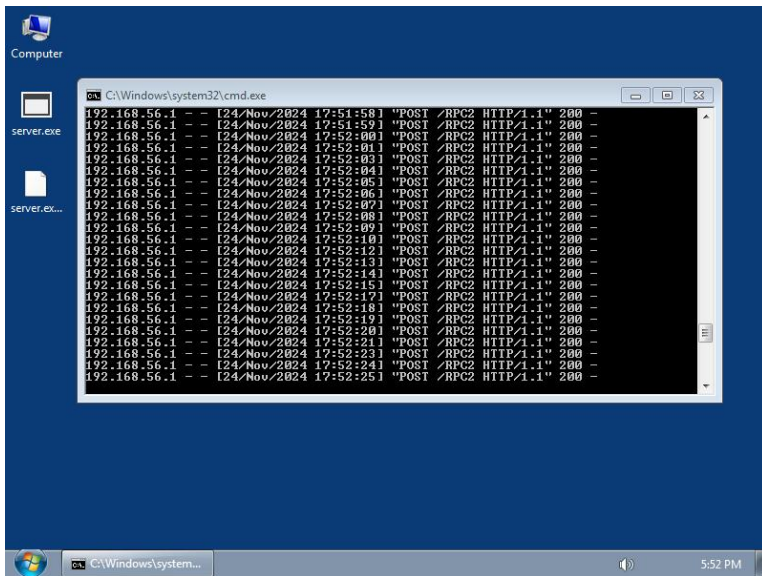
```

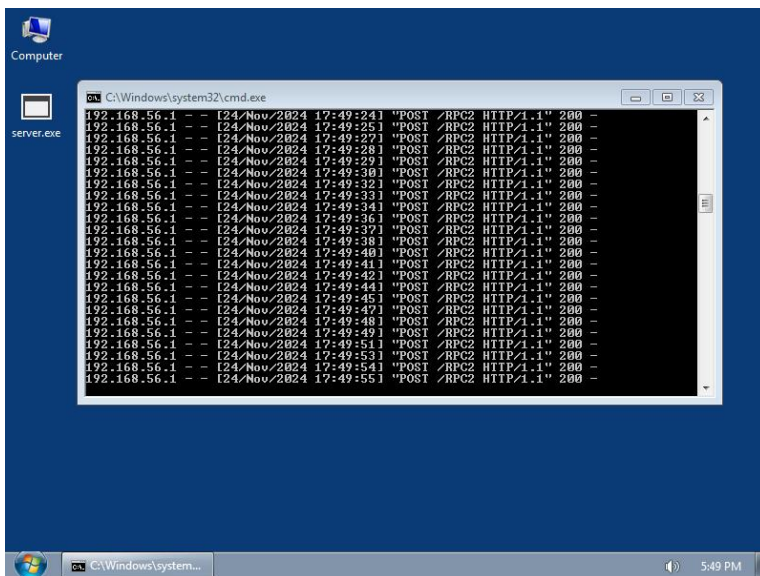
C:\Windows\system32\cmd.exe
192.168.56.1 - - [24/Nov/2024 17:50:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:30] "POST /RPC2 HTTP/1.1" 200 -
  
```

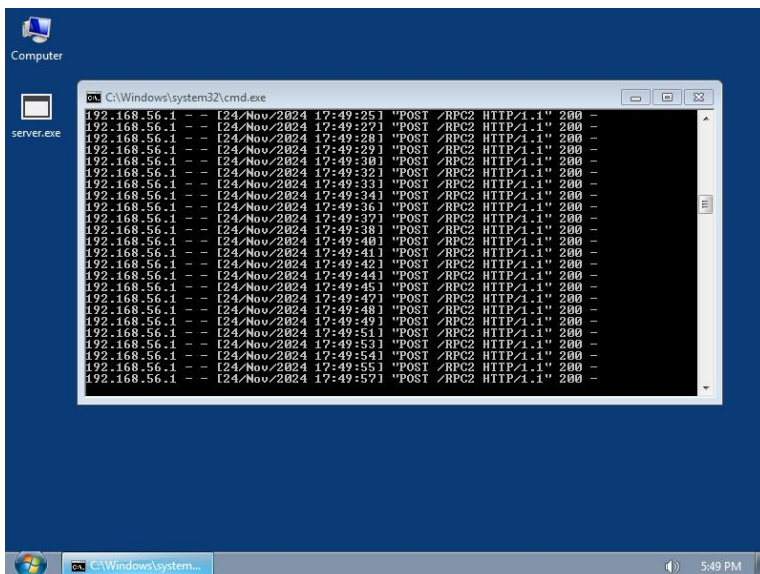
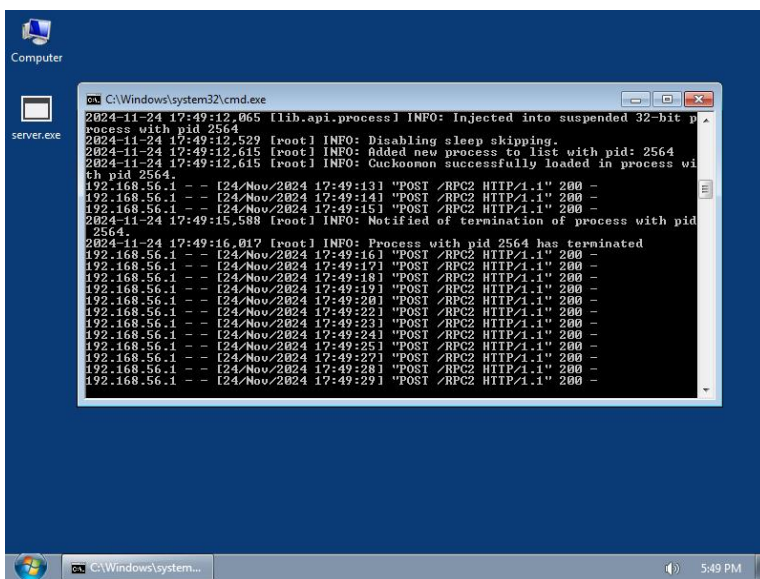
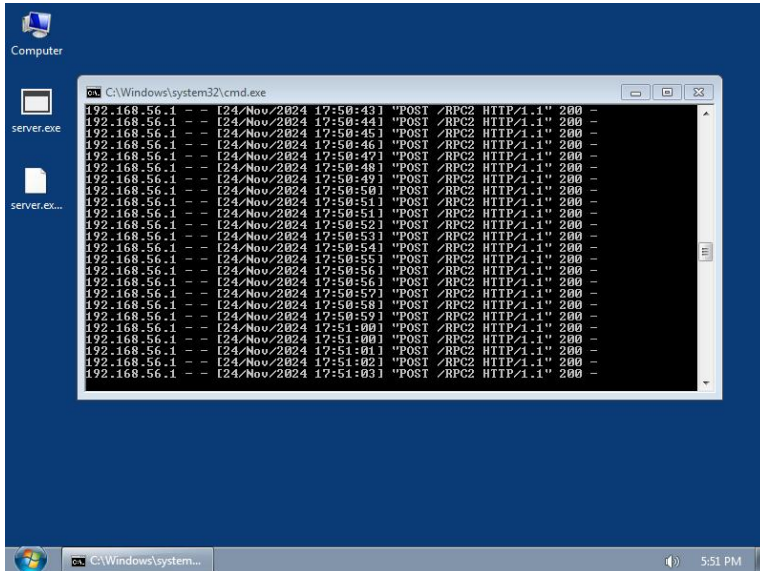


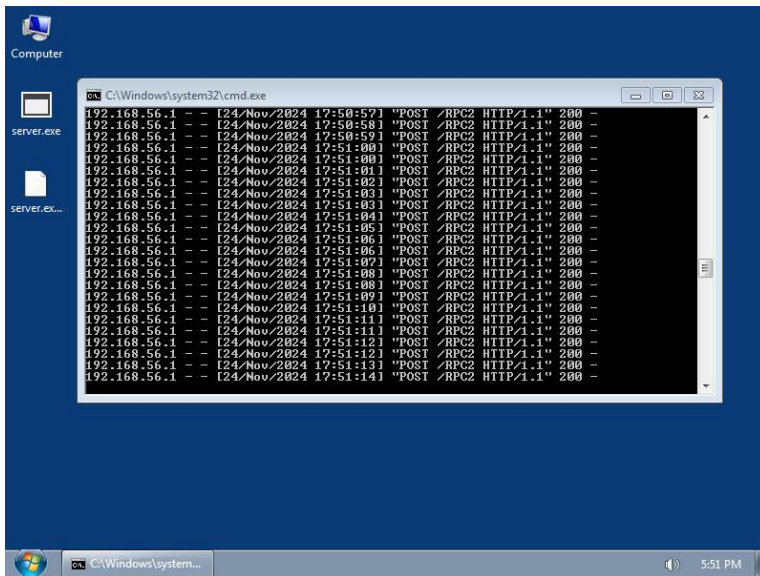
```

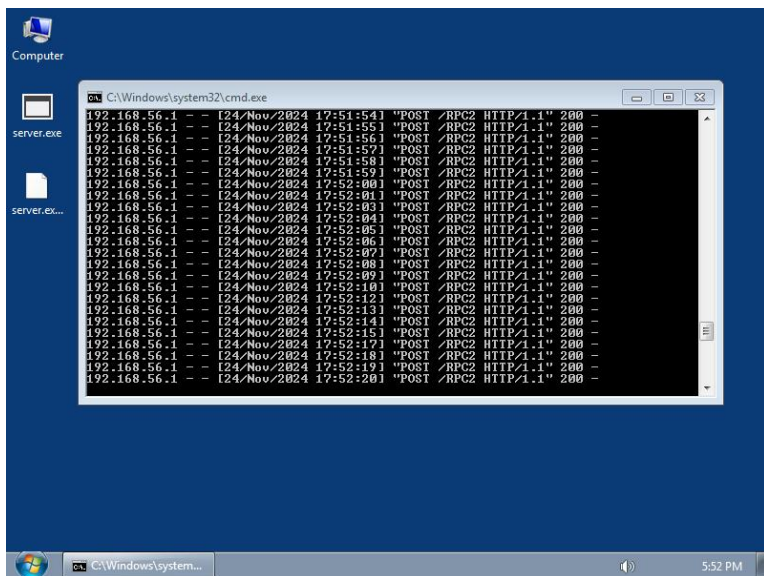
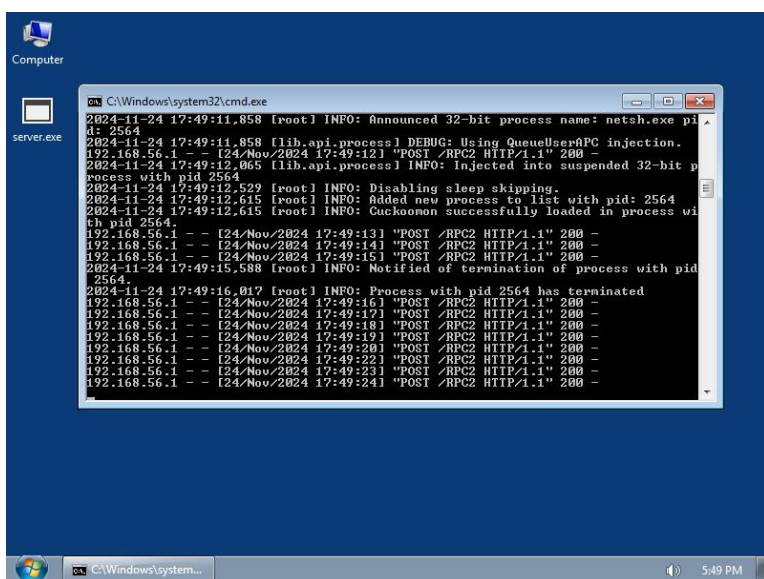
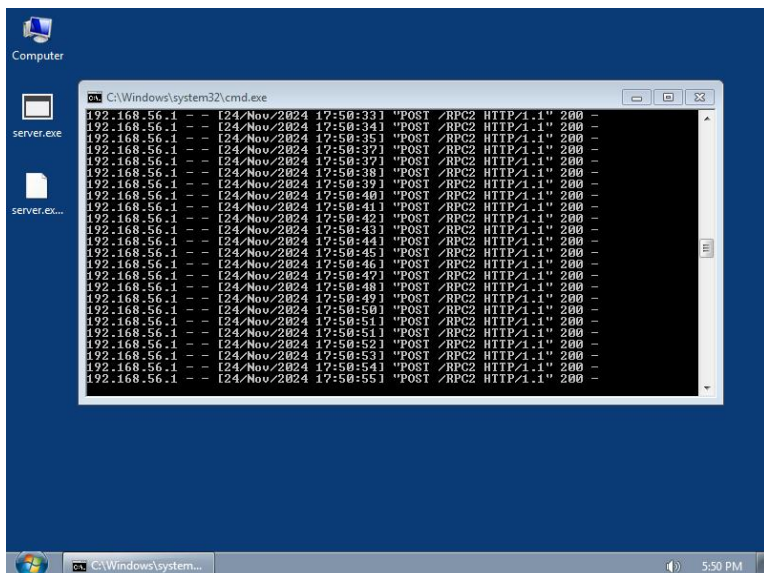
C:\Windows\system32\cmd.exe
192.168.56.1 - - [24/Nov/2024 17:52:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:52:30] "POST /RPC2 HTTP/1.1" 200 -
  
```

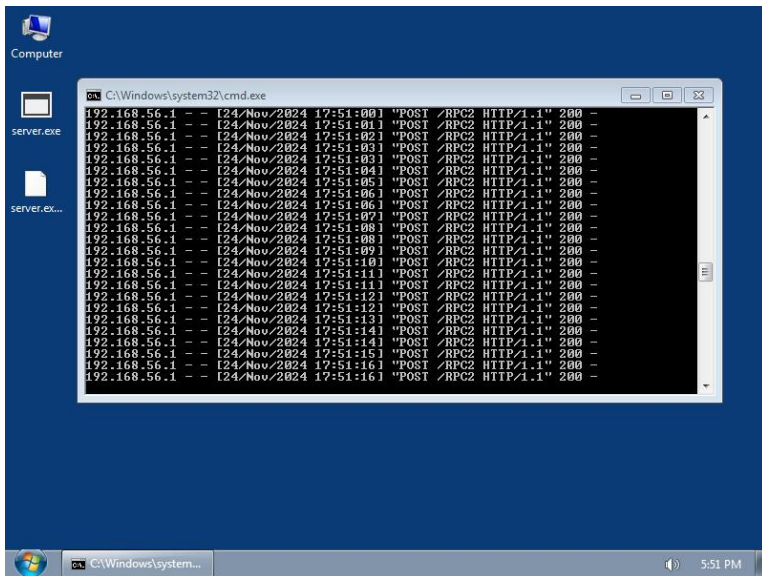



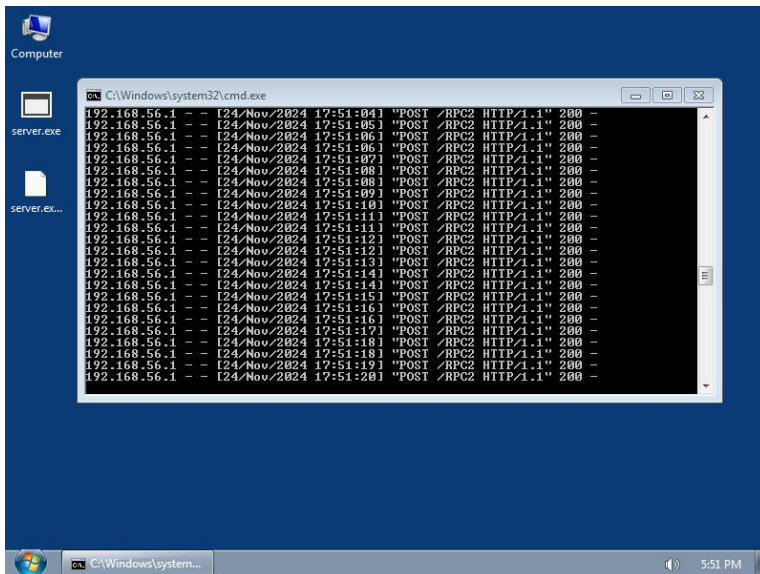






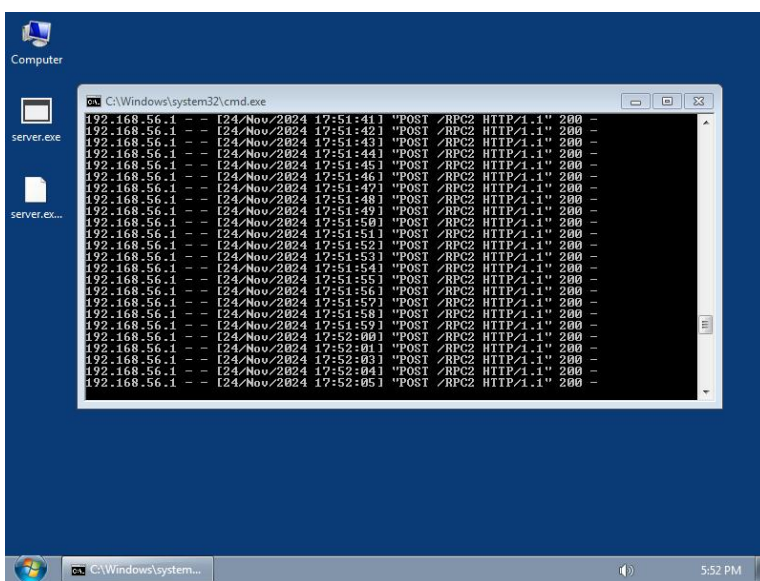






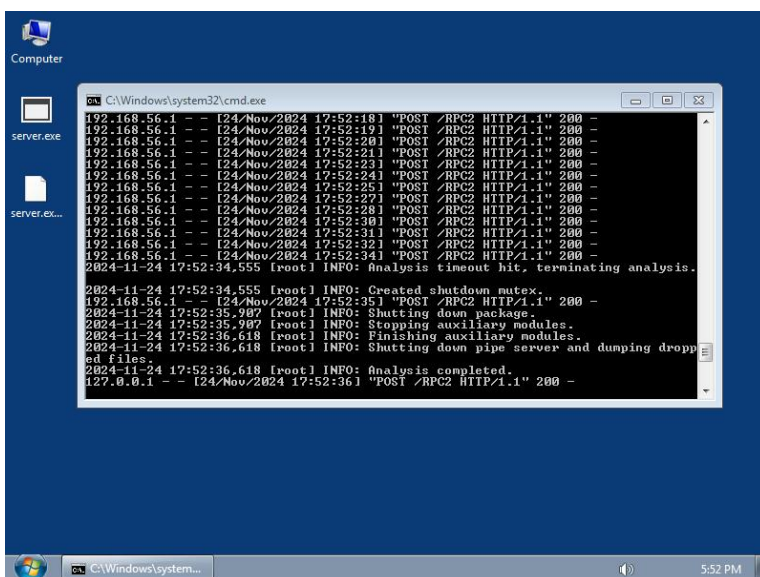
```

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:51:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:20] "POST /RPC2 HTTP/1.1" 200 -
  
```



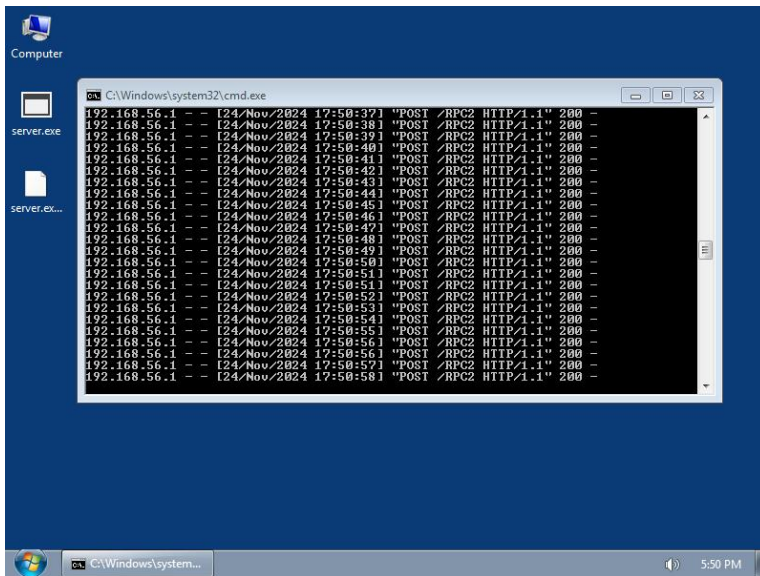
```

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:51:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:51:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:05] "POST /RPC2 HTTP/1.1" 200 -
  
```



```

C:\Windows\system32\cmd.exe
192.168.56.1 -- [24/Nov/2024 17:52:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 -- [24/Nov/2024 17:52:33] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:52:34.555 [root] INFO: Analysis timeout hit, terminating analysis.
2024-11-24 17:52:34.555 [root] INFO: Created shutdown mutex.
192.168.56.1 -- [24/Nov/2024 17:52:35] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:52:35.907 [root] INFO: Shutting down package.
2024-11-24 17:52:35.907 [root] INFO: Stopping auxiliary modules.
2024-11-24 17:52:36.618 [root] INFO: Finishing auxiliary modules.
2024-11-24 17:52:36.618 [root] INFO: Shutting down pipe server and dumping dropped files.
2024-11-24 17:52:36.618 [root] INFO: Analysis completed.
127.0.0.1 -- [24/Nov/2024 17:52:36] "POST /RPC2 HTTP/1.1" 200 -
  
```




```

Computer

C:\Windows\system32\cmd.exe

2024-11-24 17:49:06.015 [root] DEBUG: Starting analyzer from: C:\nltkckjodmu
2024-11-24 17:49:06.015 [root] DEBUG: Storing results at: C:\aZCldtMH
2024-11-24 17:49:06.015 [root] DEBUG: Pipe server name: \\.\PIPE\BiksHyyg
2024-11-24 17:49:06.015 [root] DEBUG: No analysis package specified, trying to d
etect it automatically.
2024-11-24 17:49:06.015 [root] INFO: Automatically selected analysis package "ex
s
2024-11-24 17:49:06.217 [root] DEBUG: Started auxiliary module Browser
2024-11-24 17:49:06.217 [modules.auxiliary.digisig] INFO: Skipping authenticode
validation, signtool.exe was not found in bin/
2024-11-24 17:49:06.217 [root] DEBUG: Started auxiliary module DigiSig
2024-11-24 17:49:06.217 [root] DEBUG: Started auxiliary module Disguise
2024-11-24 17:49:06.217 [root] DEBUG: Started auxiliary module Hunan
2024-11-24 17:49:06.217 [root] DEBUG: Started auxiliary module Screenshots
2024-11-24 17:49:06.217 [root] DEBUG: Started auxiliary module Usage
2024-11-24 17:49:06.250 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\User\AppData\Local\Temp\96ee36b80ad6918cdd1e5568ab9522c27cdece
a7.exe" with arguments "" with pid 2300
2024-11-24 17:49:06.250 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-11-24 17:49:06.265 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2300
192.168.56.1 - - [24/Nov/2024 17:49:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:07] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computer

server.exe

C:\Windows\system32\cmd.exe

192.168.56.1 - - [24/Nov/2024 17:51:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:37] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computer

server.exe

C:\Windows\system32\cmd.exe

192.168.56.1 - - [24/Nov/2024 17:50:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:41] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computer
server.exe

C:\Windows\system32\cmd.exe
192.168.56.1 - - [24/Nov/2024 17:49:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:10] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:11.858 [root] INFO: Announced 32-bit process name: netsh.exe pi
d: 2564
2024-11-24 17:49:11.858 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [24/Nov/2024 17:49:12] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:12.065 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2564
2024-11-24 17:49:12.529 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckoonoon successfully loaded in process wi
th pid 2564.
192.168.56.1 - - [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pid
2564.
2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 - - [24/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:49:22] "POST /RPC2 HTTP/1.1" 200 -
  
```

```

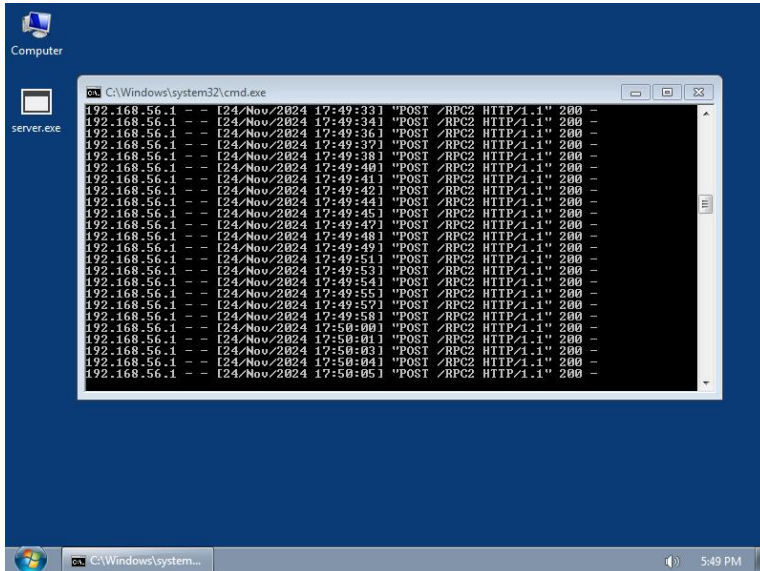
Computer
server.exe
server.ex...

C:\Windows\system32\cmd.exe
192.168.56.1 - - [24/Nov/2024 17:51:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:51:18] "POST /RPC2 HTTP/1.1" 200 -
  
```

```

Computer
server.exe
server.ex...

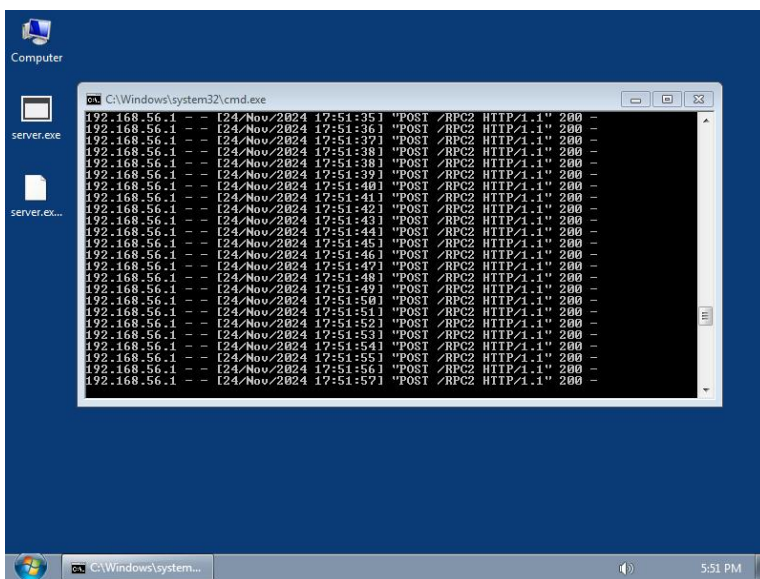
C:\Windows\system32\cmd.exe
192.168.56.1 - - [24/Nov/2024 17:50:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [24/Nov/2024 17:50:39] "POST /RPC2 HTTP/1.1" 200 -
  
```



```

C:\Windows\system32\cmd.exe
192.168.56.1 - [24/Nov/2024 17:49:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:50:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:50:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:50:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:50:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:50:05] "POST /RPC2 HTTP/1.1" 200 -

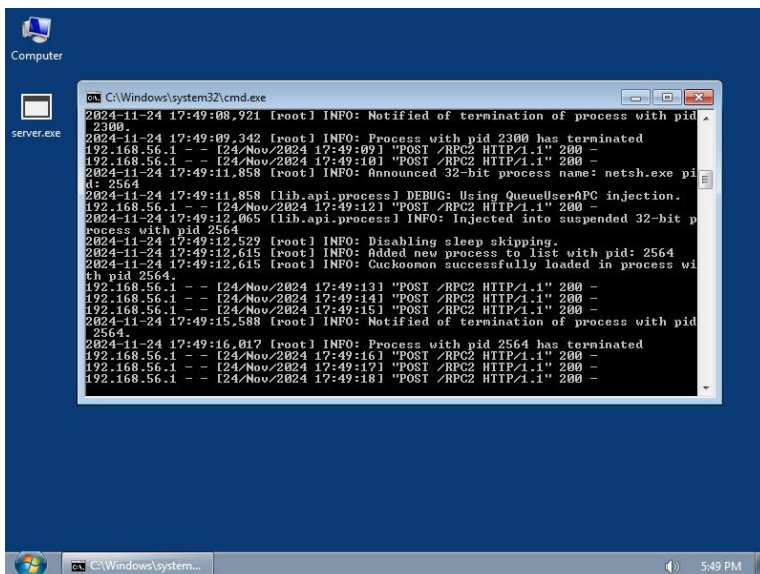
```



```

C:\Windows\system32\cmd.exe
192.168.56.1 - [24/Nov/2024 17:51:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:51:57] "POST /RPC2 HTTP/1.1" 200 -

```



```

C:\Windows\system32\cmd.exe
2024-11-24 17:49:08.921 [root] INFO: Notified of termination of process with pid 2300.
2024-11-24 17:49:09.342 [root] INFO: Process with pid 2300 has terminated
192.168.56.1 - [24/Nov/2024 17:49:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:10] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:11.858 [root] INFO: Announced 32-bit process name: netsh.exe pid: 2564
2024-11-24 17:49:11.858 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - [24/Nov/2024 17:49:12] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:12.065 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2564.
2024-11-24 17:49:12.529 [root] INFO: Disabling sleep skipping.
2024-11-24 17:49:12.615 [root] INFO: Added new process to list with pid: 2564
2024-11-24 17:49:12.615 [root] INFO: Cuckooon successfully loaded in process with pid 2564.
192.168.56.1 - [24/Nov/2024 17:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:15] "POST /RPC2 HTTP/1.1" 200 -
2024-11-24 17:49:15.588 [root] INFO: Notified of termination of process with pid 2564.
2024-11-24 17:49:16.017 [root] INFO: Process with pid 2564 has terminated
192.168.56.1 - [24/Nov/2024 17:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [24/Nov/2024 17:49:18] "POST /RPC2 HTTP/1.1" 200 -

```