VALKYRIE COMODO

Summary

File Name: GXAgMbwroieYFak.exe

File Type: PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

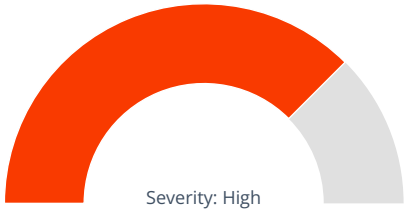
SHA1: 1d78518cc76abf62a24da3c94f1f349191ae702f

MD5: 0708b3b62998d14ef16a3bcf301ad394

MALWARE

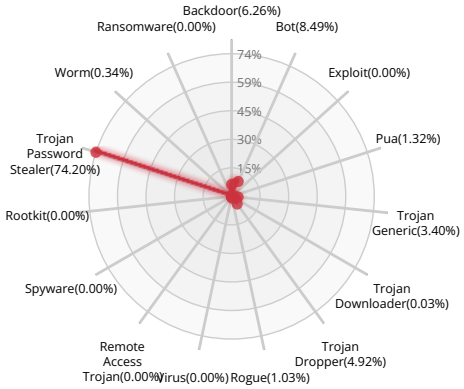
Valkyrie Final Verdict

DETECTION SECTION

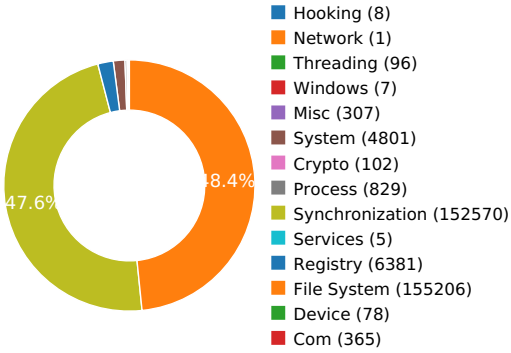


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys	Show sources

PACKER

The binary likely contains encrypted or compressed data.	Show sources

STEALING OF SENSITIVE INFORMATION

Steals private information from local Internet browsers	Show sources
Harvests credentials from local FTP client softwares	Show sources
Harvests information related to installed mail clients	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources
Executed a process and injected code into it, probably while unpacking	Show sources

DATA OBFUSCATION

Attempts to execute a powershell command with suspicious parameter/s	Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task.	Show sources
Checks the CPU name from registry, possibly for anti-virtualization	Show sources

VALKYRIE COMODO

Behavior Graph

09:57:46 **09:58:28** **09:59:10**

PID 2576

09:57:46 **Create Process** The malicious file created a child process as 1d78518cc76abf62a24da3c94f1f349191ae702f.exe **(PPID 2512)**

09:57:47 VirtualProtectEx

09:57:50 NtDelayExecution

09:58:03 CreateProcessInternal

09:58:03 Create Process

09:58:03 Create Process

09:58:03 NtResumeThread

PID 2748

09:58:05 **Create Process** The malicious file created a child process as powershell.exe **(PPID 2576)**

PID 2936

09:58:05 **Create Process** The malicious file created a child process as 1d78518cc76abf62a24da3c94f1f349191ae702f.exe **(PPID 2576)**

09:58:52 09:58:52 NtReadFile **[3 times]**

PID 556

09:58:19 **Create Process** The malicious file created a child process as svchost.exe **(PPID 452)**

PID 2556

09:58:41 **Create Process** The malicious file created a child process as WmiPrvSE.exe **(PPID 556)**

09:58:51 RegQueryValueExW

PID 2348

09:58:26 **Create Process** The malicious file created a child process as svchost.exe **(PPID 452)**

09:58:29 RegOpenKeyExW

PID 452

09:59:08 **Create Process** The malicious file created a child process as services.exe **(PPID 348)**

09:59:10 Create Process

PID 3024

09:59:10 **Create Process** The malicious file created a child process as lsass.exe **(PPID 452)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\System32\MSCOREE.DLL.local
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\Microsoft.NET\Framework*
C:\Windows\Microsoft.NET\Framework\v1.0.3705\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.0.3705\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\clr.dll
C:\Windows\Microsoft.NET\Framework\v1.1.4322\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\clr.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll
C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae702f.exe.config
C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae702f.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:\Windows\Microsoft.NET\Framework\v4.0.30319\MSVCR120_CLR0400.dll
C:\Windows\System32\MSVCR120_CLR0400.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoree.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config
C:\Windows\Microsoft.NET\Framework\v4.0.30319\fusion.localgac
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Microsoft.Net\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib*
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll.aux
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\v4.0.30319\ole32.dll
\Device\KsecDD
C:\Windows\assembly\NativeImages_v4.0.30319_32\wFpV*
C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae702f.INI
C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\GAC\PublisherPolicy.tme
C:\Windows\Microsoft.Net\assembly\GAC_32\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms*
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll.aux
C:\Windows\Microsoft.Net\assembly\GAC_32\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System*
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll.aux
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Configuration\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Configuration.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Xml\v4.0_4.0.0.0__b77a5c561934e089\System.Xml.dll
C:\Windows\Microsoft.Net\assembly\GAC_32\System.Drawing\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Drawing.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Drawing\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Drawing.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing*
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll.aux
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Security\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Security.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\Accessibility\v4.0_4.0.0.0__b03f5f7f11d50a3a\Accessibility.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Core\v4.0_4.0.0.0__b77a5c561934e089\System.Core.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Deployment\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Deployment.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Runtime.Serialization.Formatters.Soap\v4.0_4.0.0.0__b03f5f7f11d50a3a\System.Runtime.Serialization.Formatters.Soap.dll
C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\uxtheme.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\nlssorting.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\SortDefault.nlp

C:\Windows\System32\tzres.dll

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\InstallRoot

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir

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\NET Framework Setup\NDP\v4\Full\Release

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\LogResourceBinds

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\FileInUseRetryAttempts

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\FileInUseMillisecondsBetweenRetries

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek

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

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\NGen\Policy\v4.0\OptimizeUsedBinaries

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\AltJit

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\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DbgJITDebugLaunchSetting

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DbgManagedDebugger

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

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\TZI

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\MUI_Display
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\MUI_Std
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Time Zones\GTB Standard Time\MUI_Dlt
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus\FontCachePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{031E4825-7B94-4dc3-B131-E946B44C8DD5}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{04731B67-D933-450a-90E6-4ACD2E9408FE}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{11016101-E366-4D22-BC06-4ADA335C892B}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{26EE0668-A00A-44D7-9371-BEB064C98683}\SuppressionPolicy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{4336a54d-038b-4685-ab02-99bb52d3fb8b}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{450D8FBA-AD25-11D0-98A8-0800361B1103}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{5399E694-6CE5-4D6C-8FCE-1D8870FDCBA0}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{59031a47-3f72-44a7-89c5-5595fe6b30ee}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{645FF040-5081-101B-9F08-00AA002F954E}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{89D83576-6BD1-4c86-9454-BEB04E94C819}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{9343812e-1c37-4a49-a12e-4b2d810d956b}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{B4FB3F98-C1EA-428d-A78A-D1F5659CBA93}\SuppressionPolicy

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Desktop\NameSpace\{BD7A2E7B-21CB-41b2-A086-B309680C6B7E}\SuppressionPolicy

MODIFIED FILES

C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT

C:\Users\user\AppData\Local\Temp\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk

\??\PIPE\srvsvc

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\LO003FPZ5ELY42OOZN31.temp

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms

\??\PIPE\samr

C:\Windows\sysnative\wbem\repository\WRITABLE.TST

C:\Windows\sysnative\wbem\repository\MAPPING1.MAP

C:\Windows\sysnative\wbem\repository\MAPPING2.MAP

C:\Windows\sysnative\wbem\repository\MAPPING3.MAP

C:\Windows\sysnative\wbem\repository\OBJECTS.DATA

C:\Windows\sysnative\wbem\repository\INDEX.BTR

\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER

\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM

\??\WMIDataDevice

RESOLVED APIS

advapi32.dll.RegOpenKeyExW

advapi32.dll.RegQueryInfoKeyW

advapi32.dll.RegEnumKeyExW

advapi32.dll.RegEnumValueW

advapi32.dll.RegCloseKey

advapi32.dll.RegQueryValueExW

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

shlwapi.dll.UrlIsW

version.dll.GetFileVersionInfoSizeW

version.dll.GetFileVersionInfoW

version.dll.VerQueryValueW

clr.dll.SetRuntimeInfo

clr.dll._CorExeMain

mscoree.dll.CreateConfigStream
mscoreei.dll.CreateConfigStream
kernel32.dll.GetNumaHighestNodeNumber
kernel32.dll.GetSystemWindowsDirectoryW
advapi32.dll.AllocateAndInitializeSid
advapi32.dll.OpenProcessToken
advapi32.dll.GetTokenInformation
advapi32.dll.InitializeAcl
advapi32.dll.AddAccessAllowedAce
advapi32.dll.FreeSid
kernel32.dll.AddSIDToBoundaryDescriptor
kernel32.dll.CreateBoundaryDescriptorW
kernel32.dll.CreatePrivateNamespaceW
kernel32.dll.OpenPrivateNamespaceW
kernel32.dll.DeleteBoundaryDescriptor
kernel32.dll.WerRegisterRuntimeExceptionModule
kernel32.dll.RaiseException
mscoree.dll.#24
mscoreei.dll.#24
ntdll.dll.NtSetSystemInformation
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
kernel32.dll.GetNativeSystemInfo
ole32.dll.CoInitializeEx
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
ole32.dll.CoGetContextToken
clrjit.dll.sxsJitStartup
clrjit.dll.getJit

DELETED FILES

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\LO003FPZ5ELY42OOZN31.temp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.2748.32803671
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.2748.32803671
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2748.32803671

DELETED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName

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\Wow6432Node\Microsoft\.NETFramework\CLRLoadLogDir
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\v4.0.30319
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Fusion\NoClientChecks
HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\v4.0.30319\SKUs\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319\SKUs\default
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\NET Framework Setup\NDP\v4\Full\Release
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\DisableConfigCache
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\1d78518cc76abf62a24da3c94f1f349191ae702f.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\LogResourceBinds
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\FileInUseRetryAttempts
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\FileInUseMillisecondsBetweenRetries
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\UseLegacyIdentityFormat
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\DisableMSIPeek

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\NGen\Policy\v4.0
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\NGen\Policy\v4.0\OptimizeUsedBinaries
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\Servicing
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\Software\Microsoft\StrongName
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\OLEAUT
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\AltJit
HKEY_LOCAL_MACHINE\Software\Microsoft\Fusion\PublisherPolicy\Default
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\PublisherPolicy\Default\v4.0_policy.4.0.System.Windows.Forms__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Windows.Forms__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Configuration__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Configuration__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Xml__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Xml__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Drawing__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Drawing__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Security__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Security__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.Accessibility__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.Accessibility__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Core__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Core__b77a5c561934e089
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Deployment__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Deployment__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\v4.0_policy.4.0.System.Runtime.Serialization.Formatters.Soap__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Fusion\PublisherPolicy\Default\policy.4.0.System.Runtime.Serialization.Formatters.Soap__b03f5f7f11d50a3a
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\Policy\APTCA
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide

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

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1

EXECUTED COMMANDS

"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae702f.exe"

powershell Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae702f.exe"

C:\Windows\system32\lsass.exe

READ FILES

C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll

C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae702f.exe.config

C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae702f.exe

C:\Windows\Microsoft.NET\Framework\v4.0.30319\clr.dll

C:\Windows\System32\MSVCR120_CLR0400.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config

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

C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\225759bb87c854c0fff27b1d84858c21\mscorlib.ni.dll

\Device\KsecDD

C:\Windows\Microsoft.NET\Framework\v4.0.30319\clrjit.dll

C:\Windows\assembly\pubpol20.dat

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System\52cca48930e580e3189eac47158c20be\System.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\646b4b01cb29986f8e076aa65c9e9753\System.Drawing.ni.dll

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\5aac750b35b27770dccb1a43f83cced7\System.Windows.Forms.ni.dll

C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Windows.Forms\v4.0_4.0.0.0__b77a5c561934e089\System.Windows.Forms.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\nlssorting.dll

C:\Windows\Microsoft.NET\Framework\v4.0.30319\SortDefault.nlp

C:\Windows\System32\tzres.dll

C:\Windows\System32\en-US\tzres.dll.mui

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\55560c2014611e9119f99923c9ebdeef\System.Core.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\55560c2014611e9119f99923c9ebdeef\System.Core.ni.dll

C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7601.17514_none_72d18a4386696c80\GdiPlus.dll
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Windows\Fonts\tahoma.ttf
C:\Windows\Fonts\msjh.ttf
C:\Windows\Fonts\msyh.ttf
C:\Windows\Fonts\malgun.ttf
C:\Windows\Fonts\micross.ttf
C:\Windows\Fonts\segoeui.ttf
C:\Windows\Fonts\staticcache.dat
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\4695703083096416564b52b0696c5d9\System.Configuration.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\4695703083096416564b52b0696c5d9\System.Configuration.ni.dll
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\d86b080a37c60a872c82b912a2a63dac\System.Xml.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\d86b080a37c60a872c82b912a2a63dac\System.Xml.ni.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscorrc.dll
C:\Windows\Fonts\segoeuib.ttf
C:\Windows\Fonts\segoeuii.ttf
C:\Windows\Fonts\segoeuiz.ttf
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\7ca6a7b9413844e82108a9d62f88a2d9\Microsoft.VisualBasic.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\7ca6a7b9413844e82108a9d62f88a2d9\Microsoft.VisualBasic.ni.dll
C:\Windows\SysWOW64\shell32.dll
C:\Windows\SysWOW64\ieframe.dll
C:\
C:\Windows
C:\Windows\System32
C:\Windows\System32\WindowsPowerShell
C:\Windows\System32\WindowsPowerShell\v1.0
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004c.db
C:\Users\user\Desktop\desktop.ini
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\4dfa27fdd6a4cce26f99585e1c744f9b\System.Management.ni.dll.aux
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\4dfa27fdd6a4cce26f99585e1c744f9b\System.Management.ni.dll
C:\Windows\Microsoft.NET\Framework\v4.0.30319\wminet_utils.dll
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini
C:\Users\user\AppData\Roaming\Mozilla\SeaMonkey\profiles.ini
C:\Users\user\AppData\Roaming\Thunderbird\profiles.ini
C:\Users\user\AppData\Roaming\NETGATE Technologies\BlackHawk\profiles.ini
C:\Users\user\AppData\Roaming\8pecxstudios\Cyberfox\profiles.ini

C:\Users\user\AppData\Roaming\K-Meleon\profiles.ini

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

C:\Users\user\AppData\Roaming\Moonchild Productions\Pale Moon\profiles.ini

C:\Users\user\AppData\Roaming\Comodo\IceDragon\profiles.ini

C:\Users\user\AppData\Roaming\Waterfox\profiles.ini

C:\Users\user\AppData\Roaming\Postbox\profiles.ini

C:\Users\user\AppData\Roaming\Flock\Browser\profiles.ini

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Security\11689060f7aa189e220cf9df9a97254e\System.Security.ni.dll.aux

C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Security\11689060f7aa189e220cf9df9a97254e\System.Security.ni.dll

C:\FTP Navigator\Ftplist.txt

C:\Users\desktop.ini

C:\Users

C:\Users\user

MUTEXES

Local\ZoneAttributeCacheCounterMutex

Local\ZonesCacheCounterMutex

Local\ZonesLockedCacheCounterMutex

Global\CLR_CASOFF_MUTEX

MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect

HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart

HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier

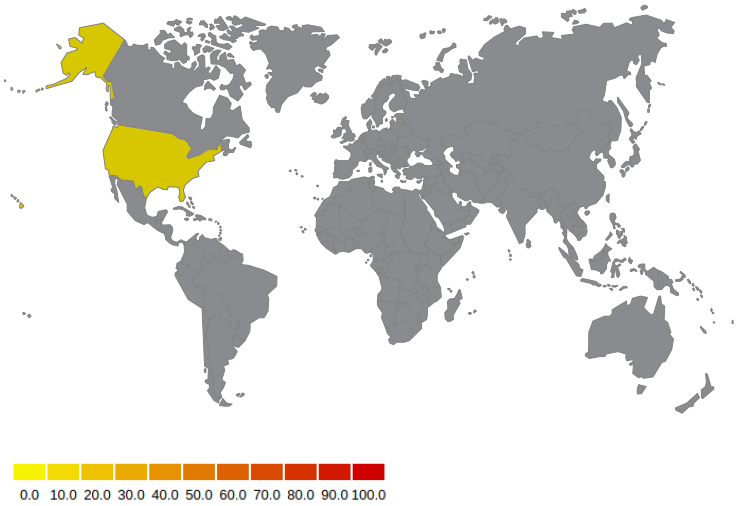
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces

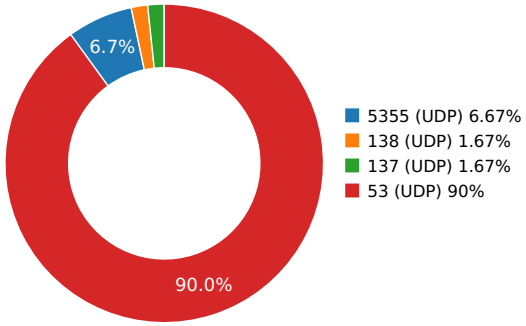
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\ESS\//./root/CIMV2\SCM Event Provider

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
www.aieov.com	45.33.2.79	United States	63949	Akamai Technologies, Inc.	Malware Process

DNS QUERIES

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

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.07139492035	Sandbox	224.0.0.252	5355
3.08084082603	Sandbox	224.0.0.252	5355
3.15124082565	Sandbox	192.168.56.255	137
4.52732086182	Sandbox	224.0.0.252	5355
5.63163590431	Sandbox	224.0.0.252	5355
7.13721394539	Sandbox	8.8.4.4	53
8.13089799881	Sandbox	8.8.8.8	53
9.14718484879	Sandbox	192.168.56.255	138
21.4912409782	Sandbox	8.8.8.8	53
22.491191864	Sandbox	8.8.4.4	53
35.8602659702	Sandbox	8.8.8.8	53
36.8505108356	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
50.8658678532	Sandbox	8.8.8.8	53
51.8655338287	Sandbox	8.8.4.4	53
65.2737588882	Sandbox	8.8.8.8	53
66.2722198963	Sandbox	8.8.4.4	53
79.7146298885	Sandbox	8.8.8.8	53
80.7093658447	Sandbox	8.8.4.4	53
98.0693118572	Sandbox	8.8.8.8	53
99.0683279037	Sandbox	8.8.4.4	53
112.441282988	Sandbox	8.8.8.8	53
113.428253889	Sandbox	8.8.4.4	53
126.847658873	Sandbox	8.8.8.8	53
127.834089994	Sandbox	8.8.4.4	53
145.107689857	Sandbox	8.8.8.8	53
146.100258827	Sandbox	8.8.4.4	53
159.472002029	Sandbox	8.8.8.8	53
160.459080935	Sandbox	8.8.4.4	53
173.86835289	Sandbox	8.8.8.8	53
174.865747929	Sandbox	8.8.4.4	53
200.870299816	Sandbox	8.8.8.8	53
201.868759871	Sandbox	8.8.4.4	53
215.225579977	Sandbox	8.8.8.8	53
216.224735975	Sandbox	8.8.4.4	53
229.585019827	Sandbox	8.8.8.8	53
230.583922863	Sandbox	8.8.4.4	53
247.834420919	Sandbox	8.8.8.8	53
248.833935022	Sandbox	8.8.4.4	53
262.194144011	Sandbox	8.8.8.8	53
263.193354845	Sandbox	8.8.4.4	53
276.553462982	Sandbox	8.8.8.8	53
277.552788019	Sandbox	8.8.4.4	53
294.804401875	Sandbox	8.8.8.8	53
295.803114891	Sandbox	8.8.4.4	53
309.162652016	Sandbox	8.8.8.8	53
310.162730932	Sandbox	8.8.4.4	53
323.522819042	Sandbox	8.8.8.8	53
324.522080898	Sandbox	8.8.4.4	53
342.873193979	Sandbox	8.8.8.8	53
343.877790928	Sandbox	8.8.4.4	53
357.228224993	Sandbox	8.8.8.8	53
358.225138903	Sandbox	8.8.4.4	53
371.584523916	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
372.584463835	Sandbox	8.8.4.4	53
505.836771965	Sandbox	8.8.8.8	53
506.834574938	Sandbox	8.8.4.4	53
520.194380999	Sandbox	8.8.8.8	53
521.193280935	Sandbox	8.8.4.4	53
534.553508043	Sandbox	8.8.8.8	53
535.553130865	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	GXAgMbwroieYFak.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
SHA1:	1d78518cc76abf62a24da3c94f1f349191ae702f
MD5:	0708b3b62998d14ef16a3bcf301ad394
First Seen Date:	2024-09-11 00:06:07.288011 (about 12 hours ago)
Number Of Clients Seen:	1
Last Analysis Date:	2024-09-11 00:06:07.288011 (about 12 hours ago)
Human Expert Analysis Date:	2024-09-11 09:51:08.151366 (about 3 hours ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	3
Trid	[[64.6, u'Win64 Executable (generic)'], [15.4, u'Win32 Dynamic Link Library (generic)'], [10.5, u'Win32 Executable (generic)'], [4.6, u'Generic Win/DOS Executable'], [4.6, u'DOS Executable Generic']]
Compilation Time Stamp	0x66DFA50D [Tue Sep 10 01:46:53 2024 UTC]
Translation	0x0000 0x04b0
LegalCopyright	\xa9 2018 Hyper V
Assembly Version	5.5.0.0
InternalName	wFpV.exe
FileVersion	5.1.0.0
CompanyName	Hyper V
LegalTrademarks	
Comments	
ProductName	Presentacion V
ProductVersion	5.1.0.0
FileDescription	Presentacion V
OriginalFilename	wFpV.exe
Entry Point	0x4b0d92 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	740872
Ssdeep	12288:hA1+h3pvL9pE1AhK31rlxlI8vyeLjr7tsoWpjOuDJiHJUd97kR:hG+LzDzKlhxaKyeXts1OuDYJUe
Sha256	8829692c411a64a87b5f857db39c8c0747b145c1cf3acb8dedad03e3bb07b62d
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/1/d/7/8/1d78518cc76abf62a24da3c94f1f349191ae702f', u'EXE:OriginalFileName': u'wFpV.exe', u'EXE:ProductName': u'Presentacion V', u'EXE:InternalName': u'wFpV.exe', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2024:09:11 00:05:38+00:00', u'EXE:InitializedDataSize': 10240, u'File:FileModifyDate': u'2024:09:11 00:05:21+00:00', u'EXE:AssemblyVersion': u'5.5.0.0', u'EXE:FileVersionNumber': u'5.1.0.0', u'EXE:FileVersion': u'5.1.0.0', u'File:FileSize': u'724 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:LegalTrademarks': u'', u'EXE:ProductVersion': u'5.1.0.0', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Hyper V', u'File:FileName': u'1d78518cc76abf62a24da3c94f1f349191ae702f', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2024:09:10 01:46:53+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'\xa9 2018 Hyper V', u'EXE:LinkerVersion': 48.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/1/d/7/8', u'EXE:FileDescription': u'Presentacion V', u'EXE:EntryPoint': u'0xb0d92', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 716288, u'EXE:Comments': u'', u'File:FileInodeChangeDate': u'2024:09:11 00:05:38+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'5.1.0.0'}]
Mime Type	application/x-dosexec
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x2000	0xaed98	0xaee00	7.86606851913	7f46c79576acb59774a95772996ae5d4
.rsrc	0xb2000	0x2548	0x2600	7.58494589727	36ecea02ba906f9a0782aa6ad86a393d
.reloc	0xb6000	0xc	0x200	0.0815394123432	71852a407d1c0ac5e68f4534f8aee4a4

PE Imports

- mscoree.dll
  - _CorExeMain

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 729288, u'sha256': u'ddae8db4092e19b7b0148f255e10afeed7dcfa50e336ab3e2f77d930f4677747', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 8475}

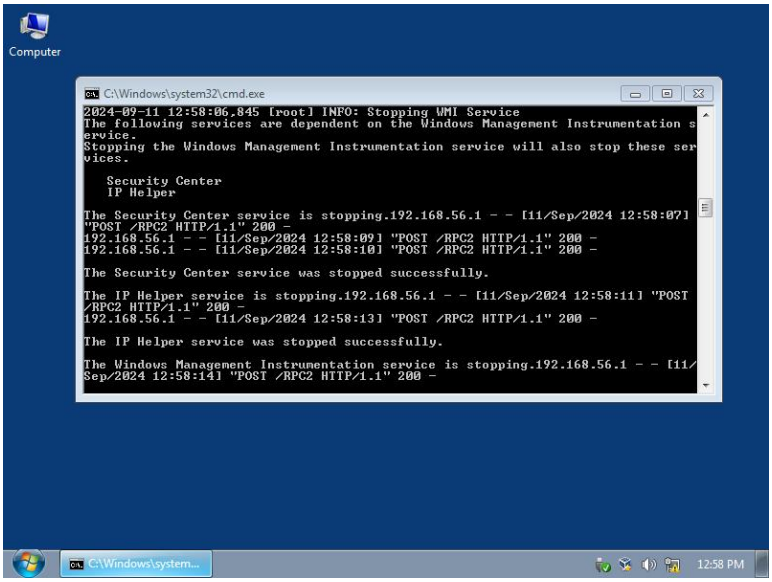
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 737780, u'sha256': u'd469742d532f7d313988545a16d67db4792d543f3b12af6a8ead461d0929406c', u'type': u'MS Windows icon resource - 1 icon, 256x256', u'size': 20}

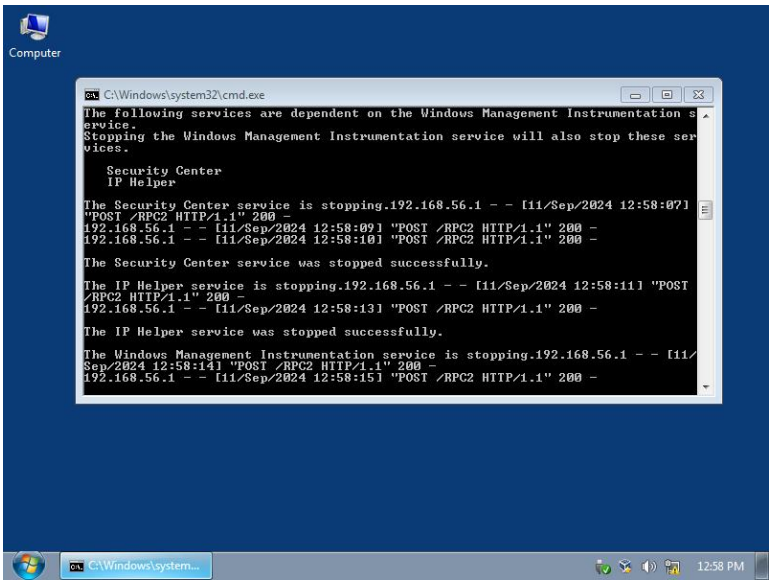
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 737816, u'sha256': u'096d4ceb875ffe56006bfb02af22c089cd9225221daaa83dec4673d39a5f5e63', u'type': u'data', u'size': 812}

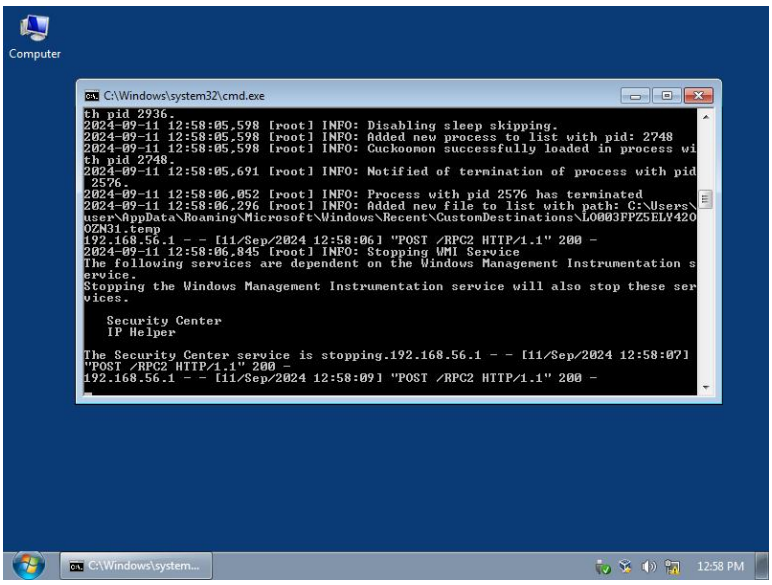
CERTIFICATE VALIDATION

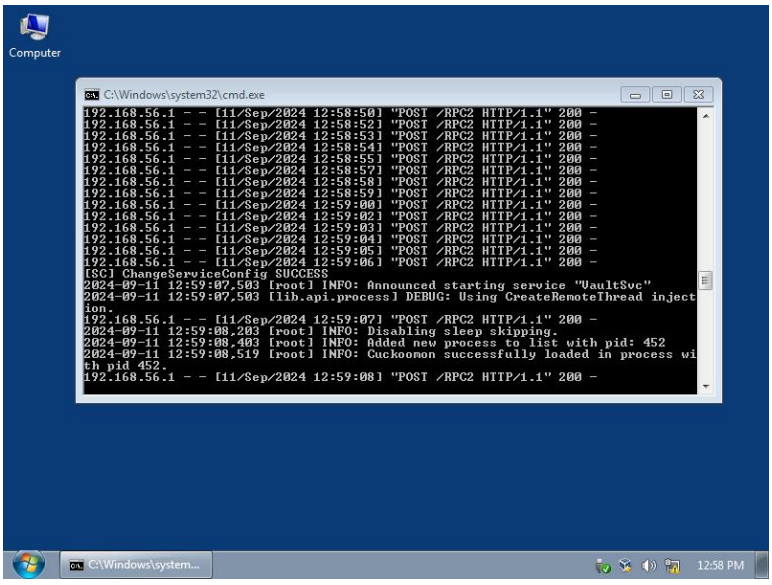
- Certificate Validation is not Applicable ?

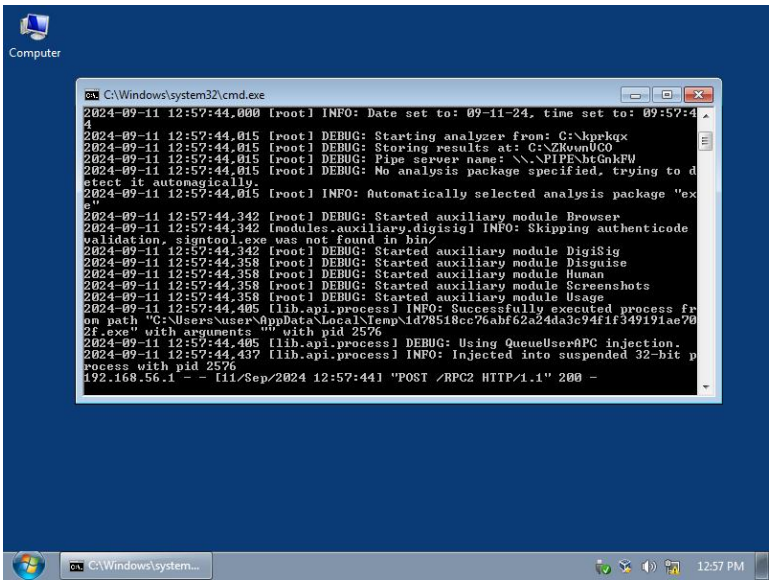
SCREENSHOTS

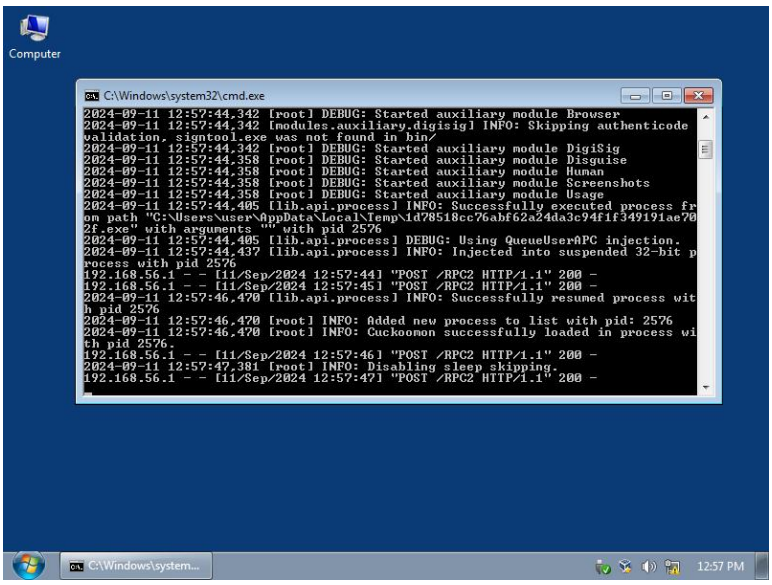


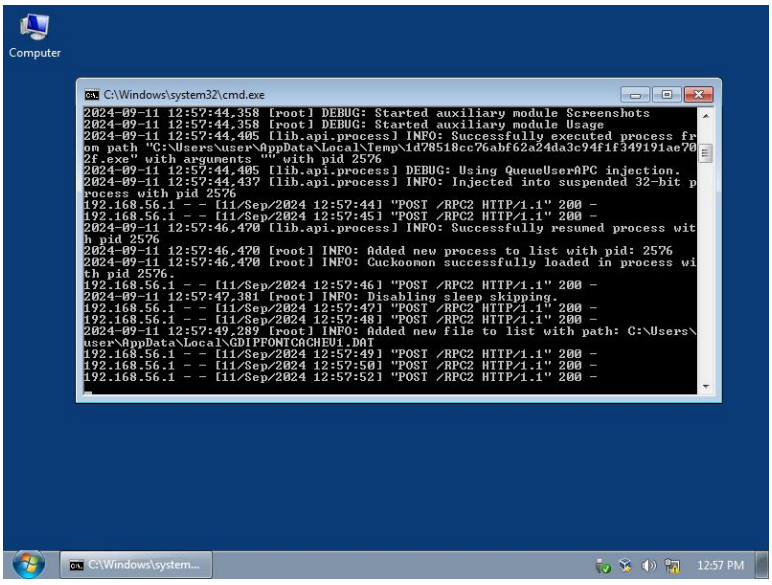

Computer
C:\Windows\system32\cmd.exe
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.
Security Center
IP Helper
The Security Center service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:10] "POST /RPC2 HTTP/1.1" 200 -
The Security Center service was stopped successfully.
The IP Helper service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:13] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:15] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

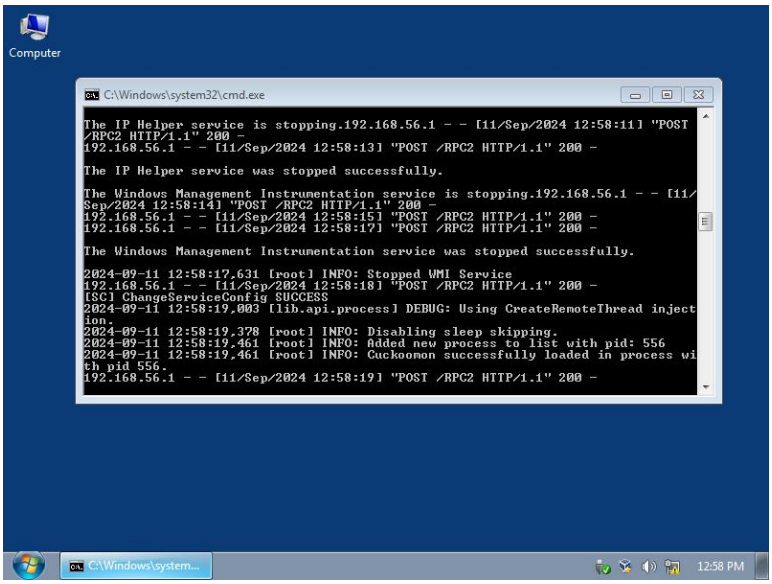

Computer
C:\Windows\system32\cmd.exe
th pid 2936.
2024-09-11 12:58:05,598 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:05,598 [root] INFO: Added new process to list with pid: 2748
2024-09-11 12:58:05,598 [root] INFO: Cuckoomon successfully loaded in process with pid 2748.
2024-09-11 12:58:05,691 [root] INFO: Notified of termination of process with pid 2576.
2024-09-11 12:58:06,052 [root] INFO: Process with pid 2576 has terminated
2024-09-11 12:58:06,296 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\LO003FPZ5ELY420OZN31.temp
192.168.56.1 - - [11/Sep/2024 12:58:06] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:06,845 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.
Security Center
IP Helper
The Security Center service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:09] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

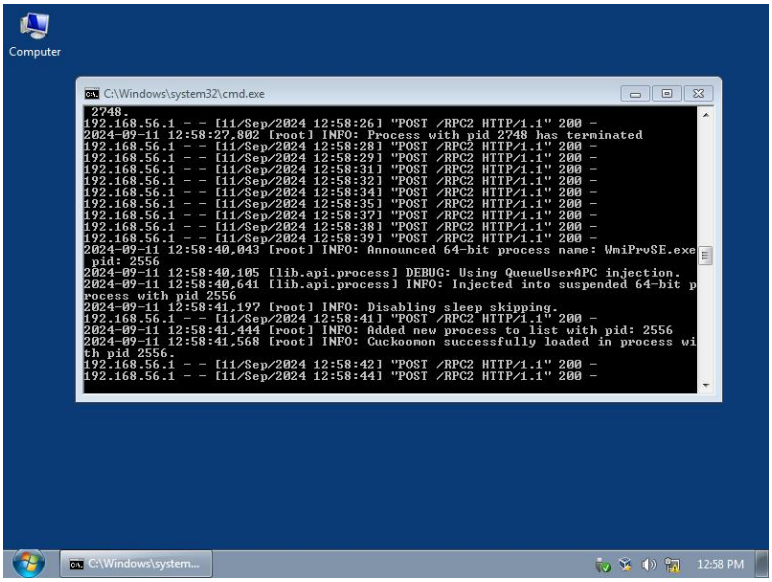

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:06] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-09-11 12:59:07,503 [root] INFO: Announced starting service "VaultSvc"
2024-09-11 12:59:07,503 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
192.168.56.1 - - [11/Sep/2024 12:59:07] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:08,203 [root] INFO: Disabling sleep skipping.
2024-09-11 12:59:08,403 [root] INFO: Added new process to list with pid: 452
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

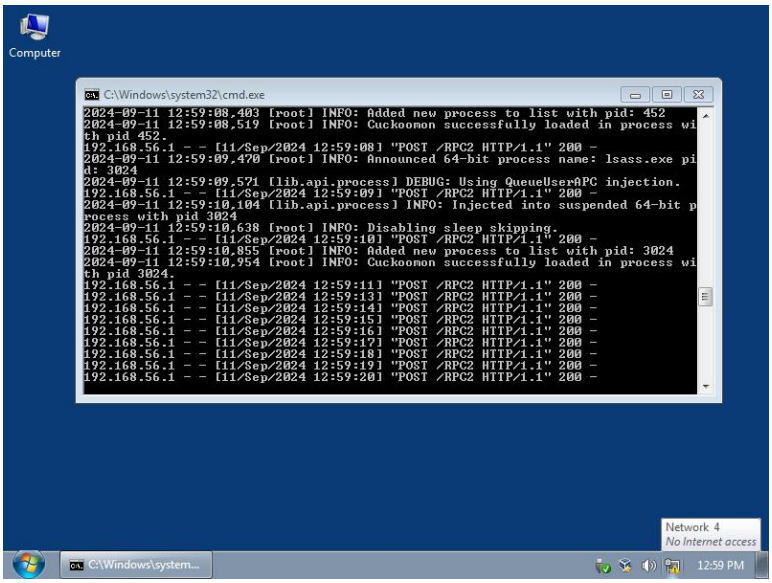

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:57:44,000 [root] INFO: Date set to: 09-11-24, time set to: 09:57:44
2024-09-11 12:57:44,015 [root] DEBUG: Starting analyzer from: C:\kprkqx
2024-09-11 12:57:44,015 [root] DEBUG: Storing results at: C:\ZKwvnUCO
2024-09-11 12:57:44,015 [root] DEBUG: Pipe server name: \\.\PIPE\btGnkFW
2024-09-11 12:57:44,015 [root] DEBUG: No analysis package specified, trying to detect it automagically.
2024-09-11 12:57:44,015 [root] INFO: Automatically selected analysis package "exe"
2024-09-11 12:57:44,342 [root] DEBUG: Started auxiliary module Browser
2024-09-11 12:57:44,342 [modules.auxiliary.digisig] INFO: Skipping authenticode validation, signtool.exe was not found in bin/
2024-09-11 12:57:44,342 [root] DEBUG: Started auxiliary module DigiSig
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Disguise
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Human
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Screenshots
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Usage
2024-09-11 12:57:44,405 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae702f.exe" with arguments "" with pid 2576
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:57 PM

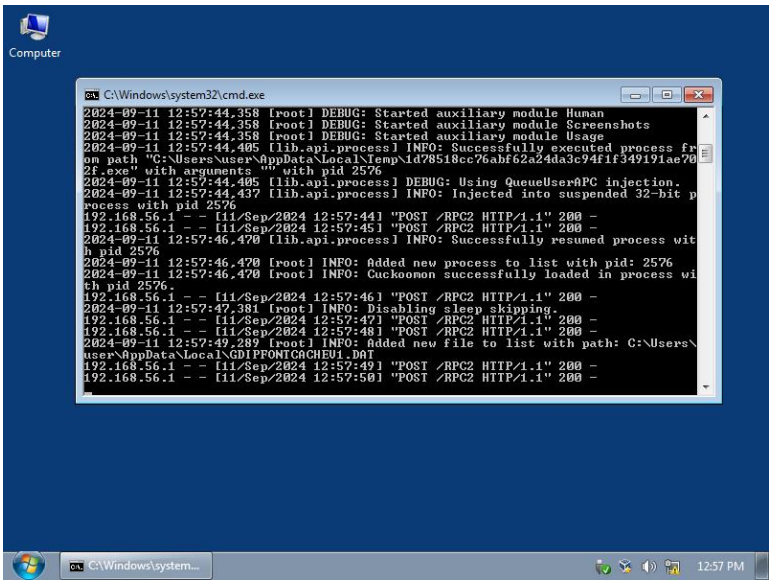

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:57:44,342 [root] DEBUG: Started auxiliary module Browser
2024-09-11 12:57:44,342 [modules.auxiliary.digisig] INFO: Skipping authenticode validation, signtool.exe was not found in bin/
2024-09-11 12:57:44,342 [root] DEBUG: Started auxiliary module DigiSig
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Disguise
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Human
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Screenshots
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Usage
2024-09-11 12:57:44,405 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae702f.exe" with arguments "" with pid 2576
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process with pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process with pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:57 PM

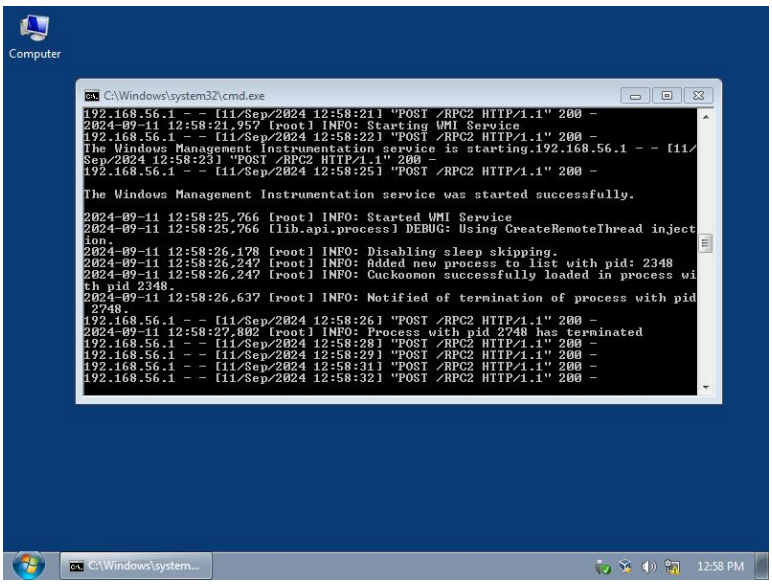

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Screenshots
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Usage
2024-09-11 12:57:44,405 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae702f.exe" with arguments "" with pid 2576
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process with pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process with pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:52] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:57 PM

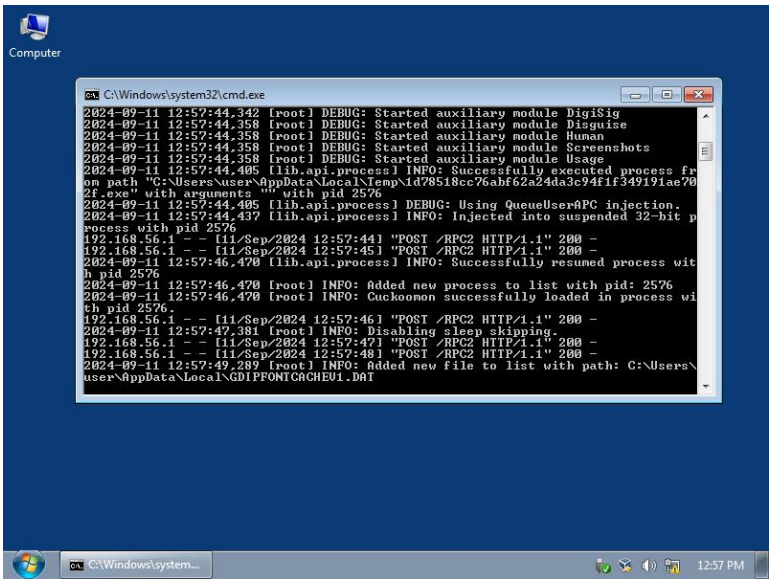

Computer
C:\Windows\system32\cmd.exe
The IP Helper service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:13] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:17] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was stopped successfully.
2024-09-11 12:58:17,631 [root] INFO: Stopped WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:18] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-09-11 12:58:19,003 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:19,378 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:19,461 [root] INFO: Added new process to list with pid: 556
2024-09-11 12:58:19,461 [root] INFO: Cuckoomon successfully loaded in process with pid 556.
192.168.56.1 - - [11/Sep/2024 12:58:19] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

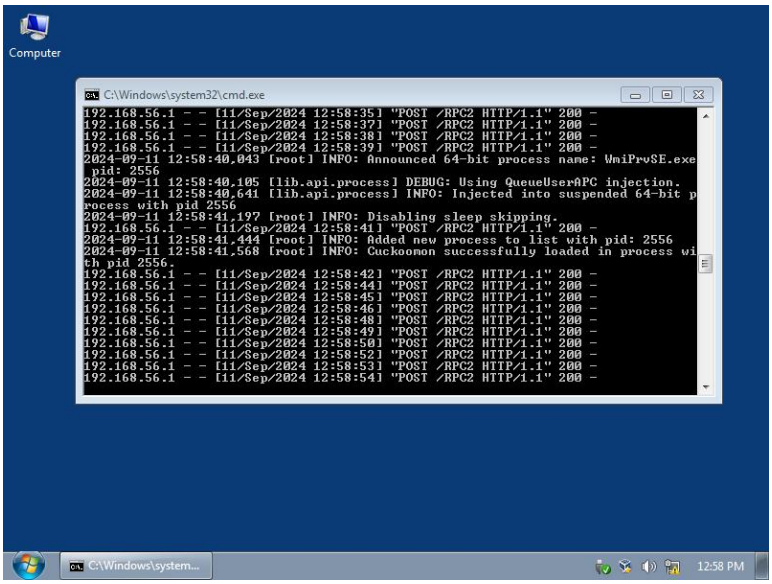

Computer
C:\Windows\system32\cmd.exe
2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

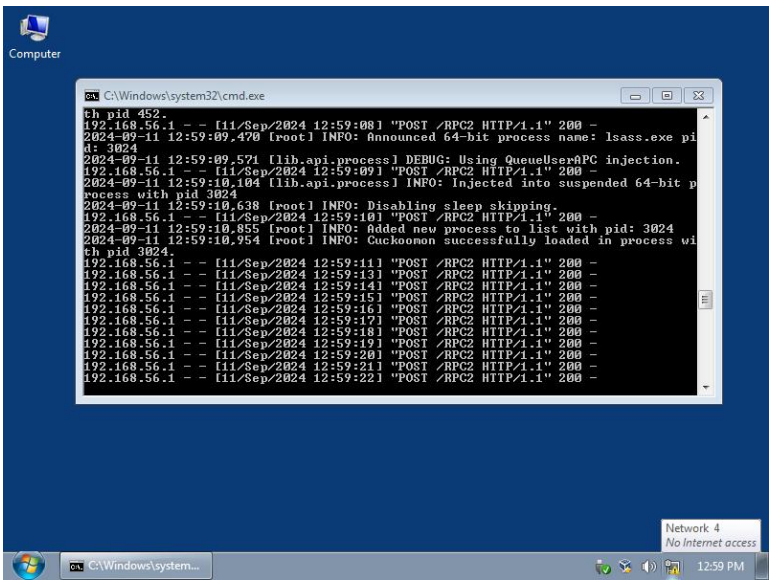

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:59:08,403 [root] INFO: Added new process to list with pid: 452
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:20] "POST /RPC2 HTTP/1.1" 200 -
Network 4
No Internet access
C:\Windows\system...
12:59 PM

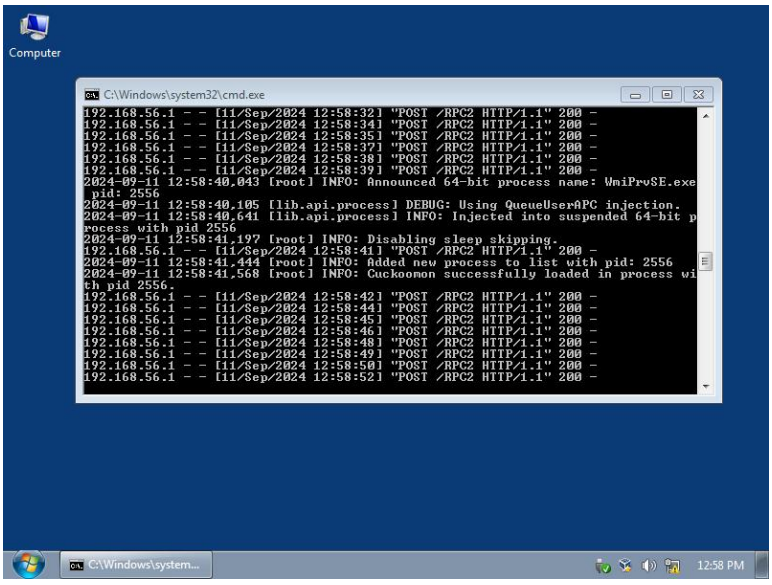

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Human
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Screenshots
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Usage
2024-09-11 12:57:44,405 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae70
2f.exe" with arguments "" with pid 2576
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process wit
h pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\GDIPFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:50] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:57 PM

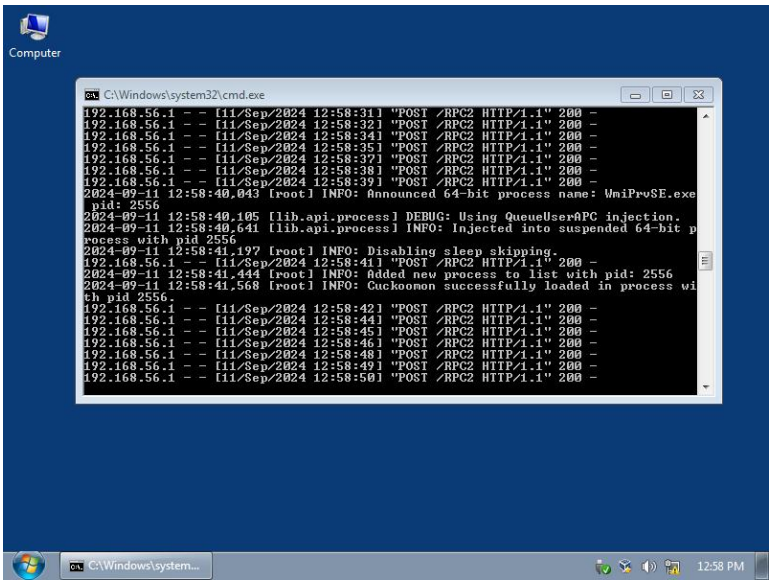

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:21] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:21,957 [root] INFO: Starting WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:22] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service is starting.192.168.56.1 - - [11/
Sep/2024 12:58:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:25] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-09-11 12:58:25,766 [root] INFO: Started WMI Service
2024-09-11 12:58:25,766 [lib.api.process] DEBUG: Using CreateRemoteThread inject
ion.
2024-09-11 12:58:26,178 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:26,247 [root] INFO: Added new process to list with pid: 2348
2024-09-11 12:58:26,247 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2348.
2024-09-11 12:58:26,637 [root] INFO: Notified of termination of process with pid
 2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

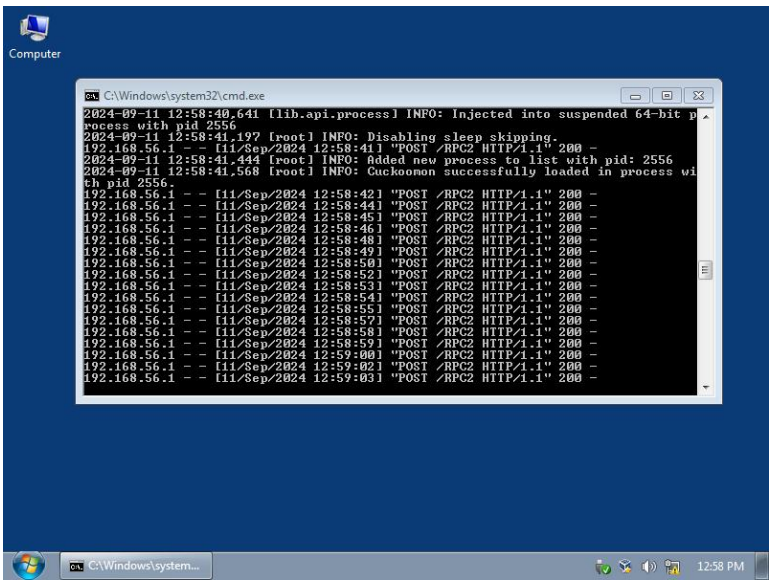

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:57:44,342 [root] DEBUG: Started auxiliary module DigiSig
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Disguise
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Human
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Screenshots
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Usage
2024-09-11 12:57:44,405 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae70
2f.exe" with arguments "" with pid 2576
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process wit
h pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\GDIPFONTCACHEV1.DAT
C:\Windows\system...
12:57 PM

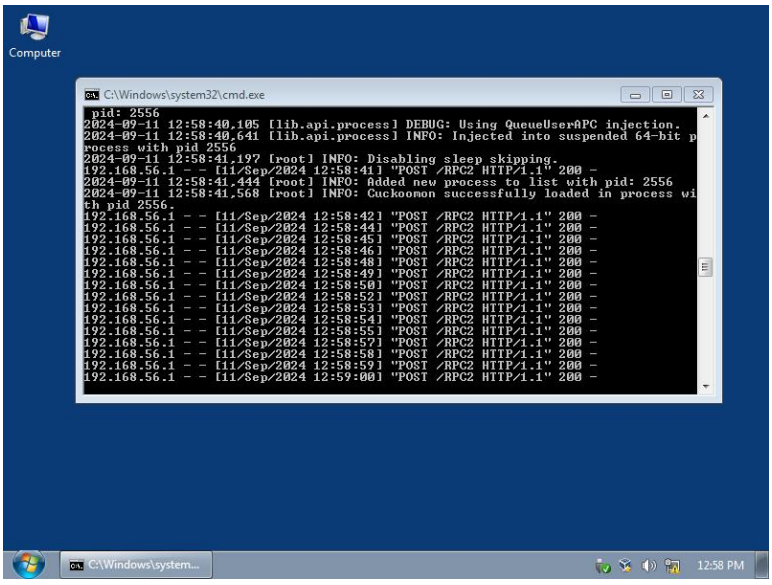

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe
pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:54] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

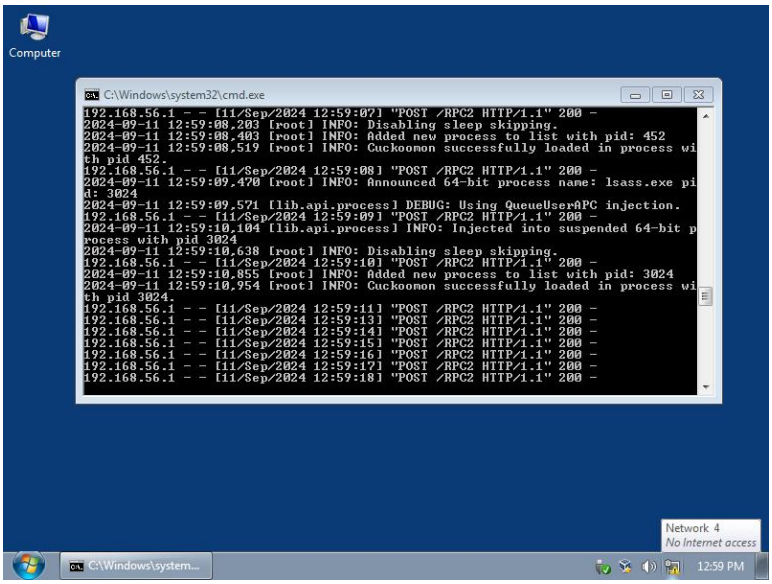

Computer
C:\Windows\system32\cmd.exe
th pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pi
d: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:22] "POST /RPC2 HTTP/1.1" 200 -
Network 4
No Internet access
C:\Windows\system...
12:59 PM

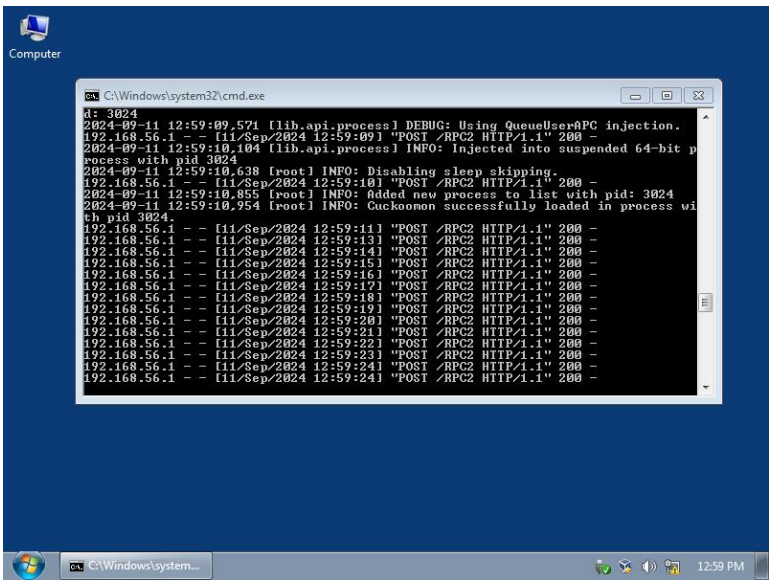

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe
pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

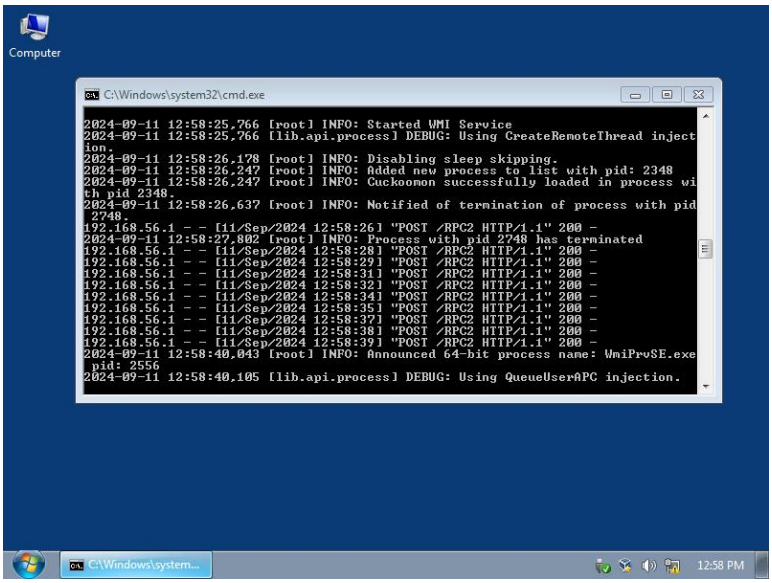

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

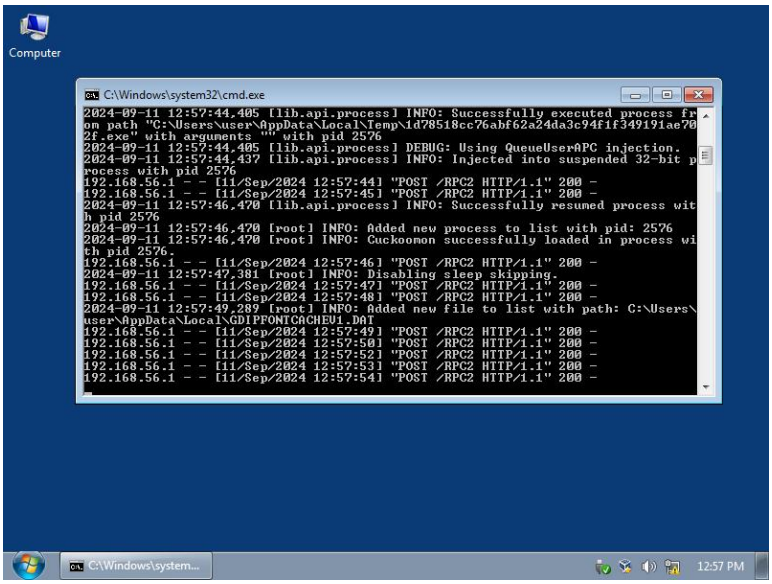

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:03] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

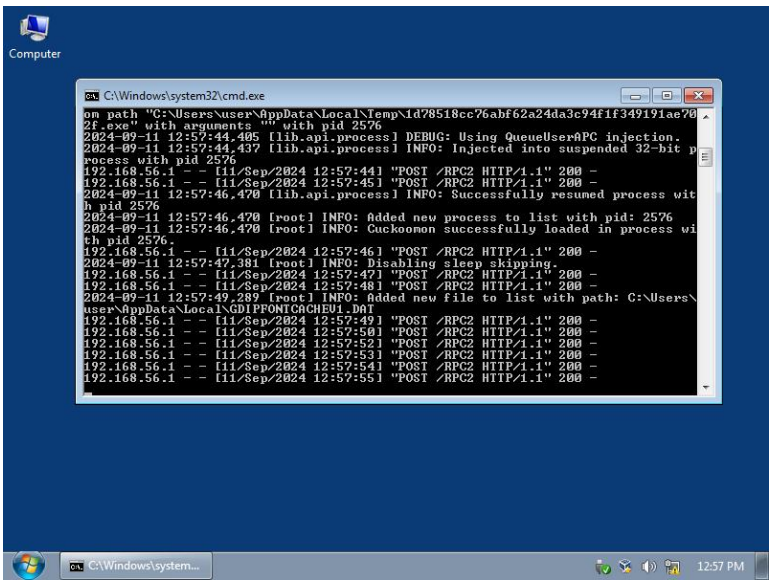

Computer
C:\Windows\system32\cmd.exe
pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:00] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

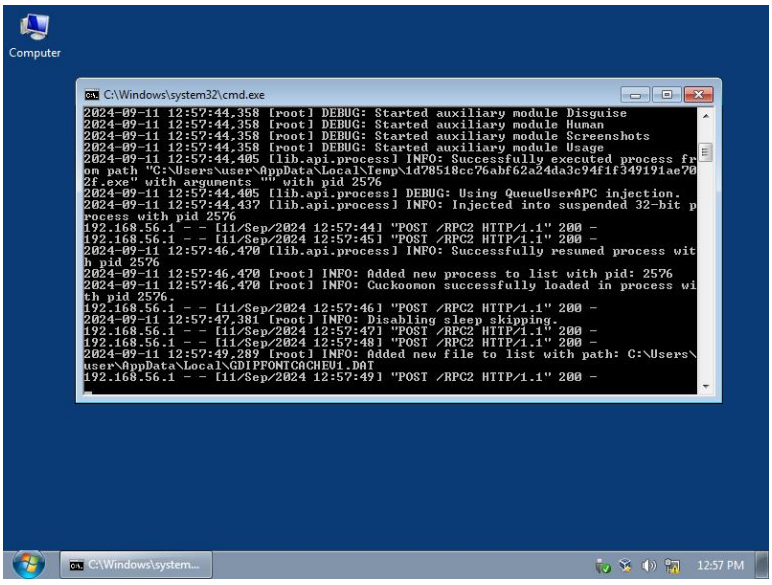

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:59:07] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:08,203 [root] INFO: Disabling sleep skipping.
2024-09-11 12:59:08,403 [root] INFO: Added new process to list with pid: 452
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:18] "POST /RPC2 HTTP/1.1" 200 -
Network 4
No Internet access
C:\Windows\system...
12:59 PM

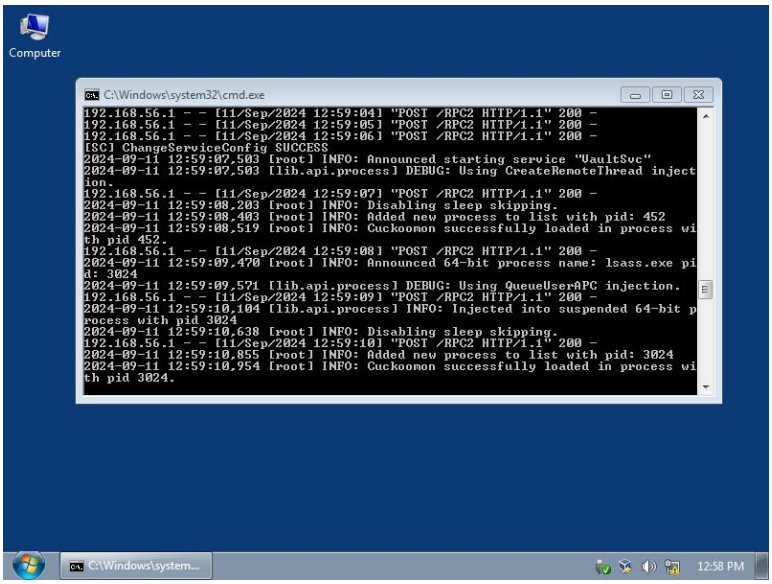

Computer
C:\Windows\system32\cmd.exe
d: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:24] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:59 PM

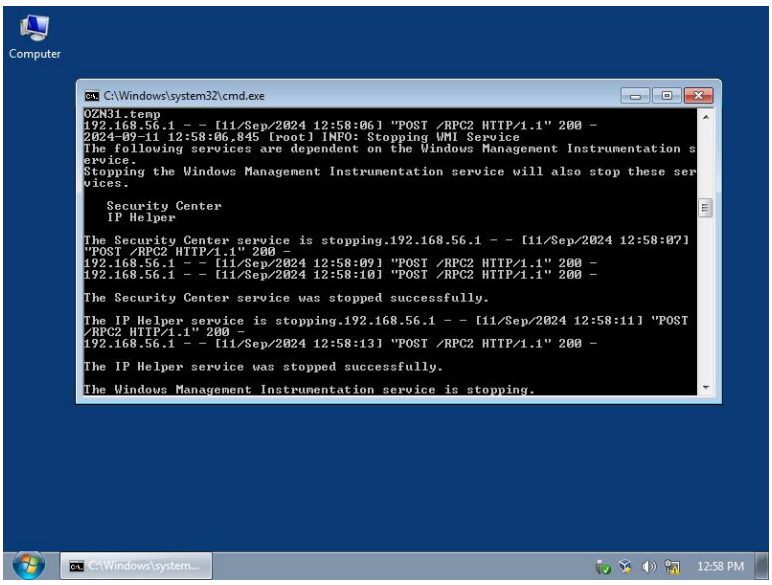

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:25,766 [root] INFO: Started WMI Service
2024-09-11 12:58:25,766 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:26,178 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:26,247 [root] INFO: Added new process to list with pid: 2348
2024-09-11 12:58:26,247 [root] INFO: Cuckoomon successfully loaded in process with pid 2348.
2024-09-11 12:58:26,637 [root] INFO: Notified of termination of process with pid 2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
C:\Windows\system...
12:58 PM

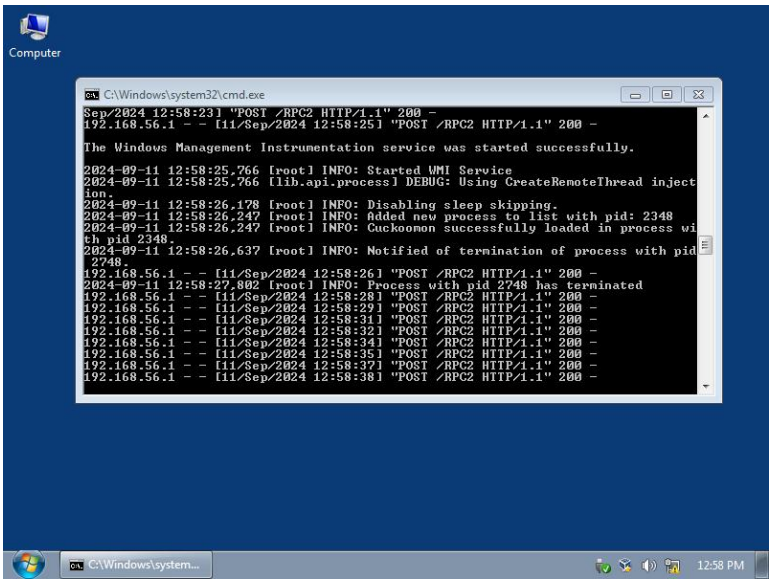

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:57:44,405 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae70
2f.exe" with arguments "" with pid 2576
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process wit
h pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\GDIPFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:54] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:57 PM

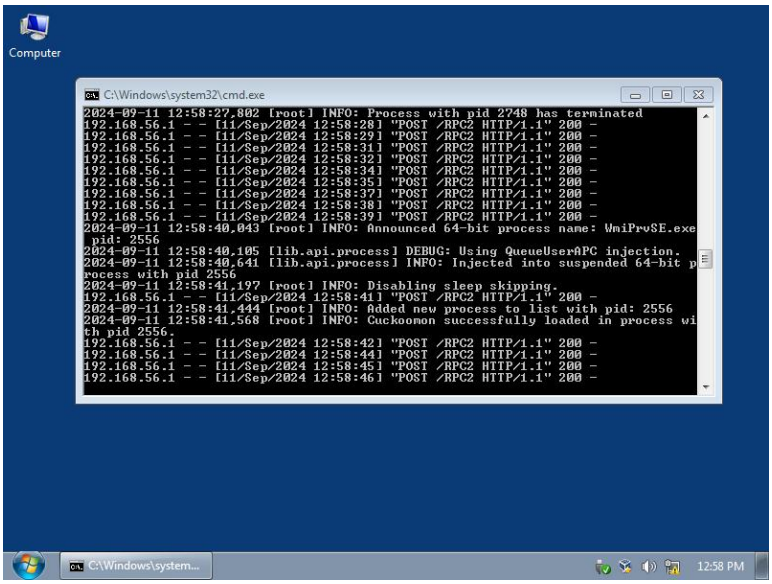

Computer
C:\Windows\system32\cmd.exe
om path "C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae70
2f.exe" with arguments "" with pid 2576
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process wit
h pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\GDIPFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:55] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:57 PM

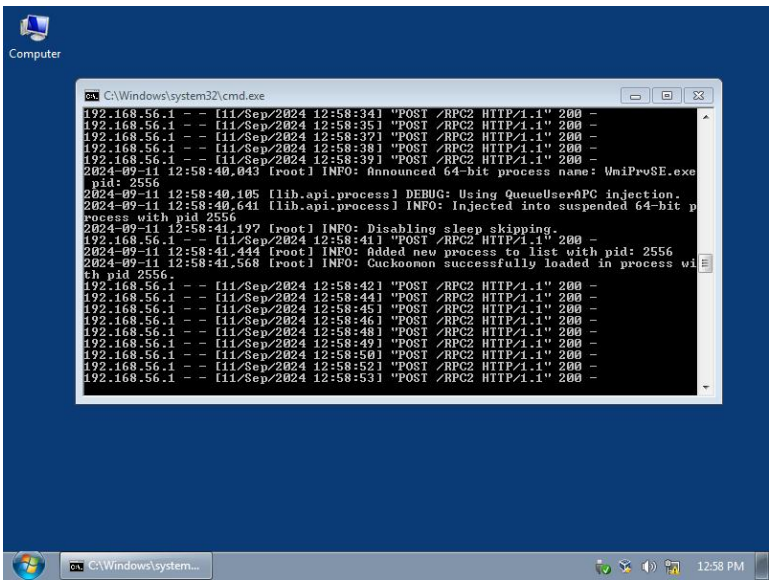

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Disguise
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Human
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Screenshots
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Usage
2024-09-11 12:57:44,405 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae70
2f.exe" with arguments "" with pid 2576
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process wit
h pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\GDIPFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:57 PM

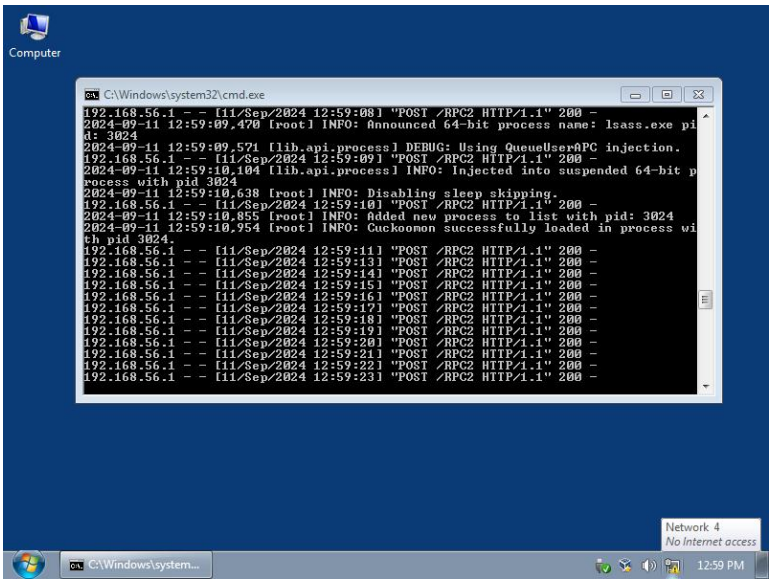

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:59:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:06] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-09-11 12:59:07,503 [root] INFO: Announced starting service "VaultSvc"
2024-09-11 12:59:07,503 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
192.168.56.1 - - [11/Sep/2024 12:59:07] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:08,203 [root] INFO: Disabling sleep skipping.
2024-09-11 12:59:08,403 [root] INFO: Added new process to list with pid: 452
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
C:\Windows\system...
12:58 PM

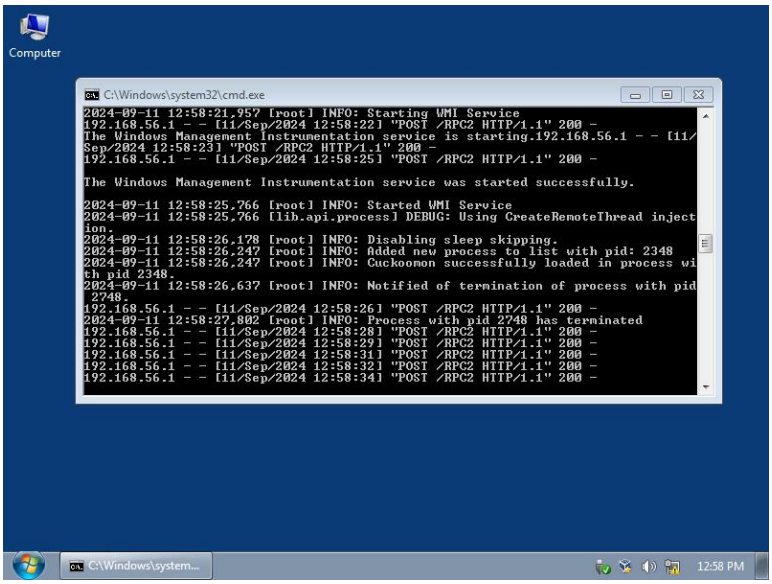

Computer
C:\Windows\system32\cmd.exe
OZN31.temp
192.168.56.1 - - [11/Sep/2024 12:58:06] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:06,845 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.
Security Center
IP Helper
The Security Center service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:10] "POST /RPC2 HTTP/1.1" 200 -
The Security Center service was stopped successfully.
The IP Helper service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:13] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.
C:\Windows\system...
12:58 PM

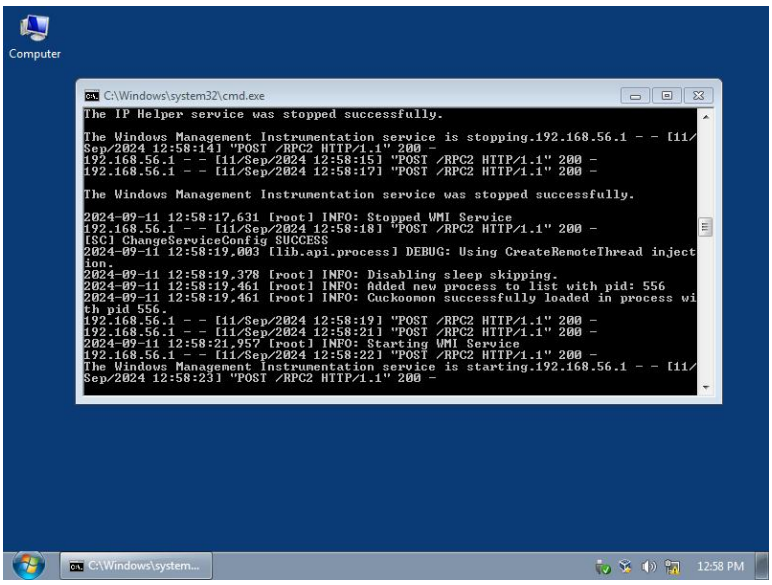

Computer
C:\Windows\system32\cmd.exe
Sep/2024 12:58:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:25] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-09-11 12:58:25,766 [root] INFO: Started WMI Service
2024-09-11 12:58:25,766 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:26,178 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:26,247 [root] INFO: Added new process to list with pid: 2348
2024-09-11 12:58:26,247 [root] INFO: Cuckoomon successfully loaded in process with pid 2348.
2024-09-11 12:58:26,637 [root] INFO: Notified of termination of process with pid 2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

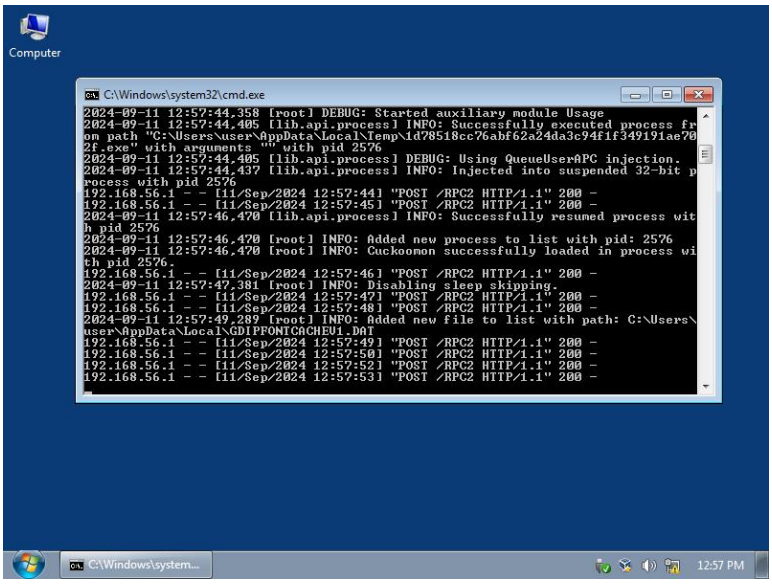

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

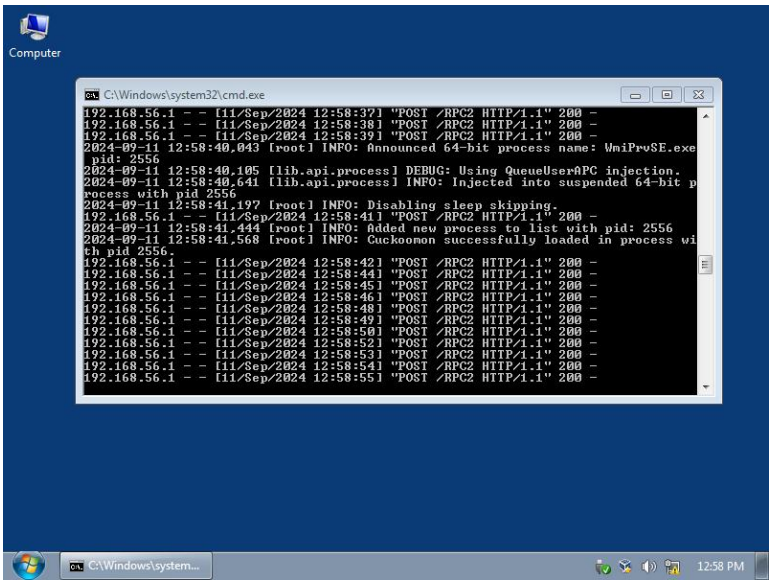

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

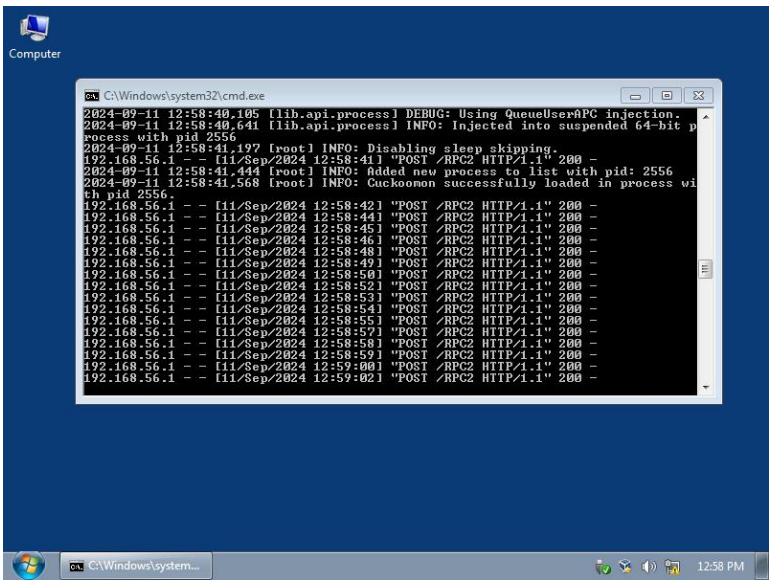

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:23] "POST /RPC2 HTTP/1.1" 200 -
Network 4
No Internet access
C:\Windows\system...
12:59 PM

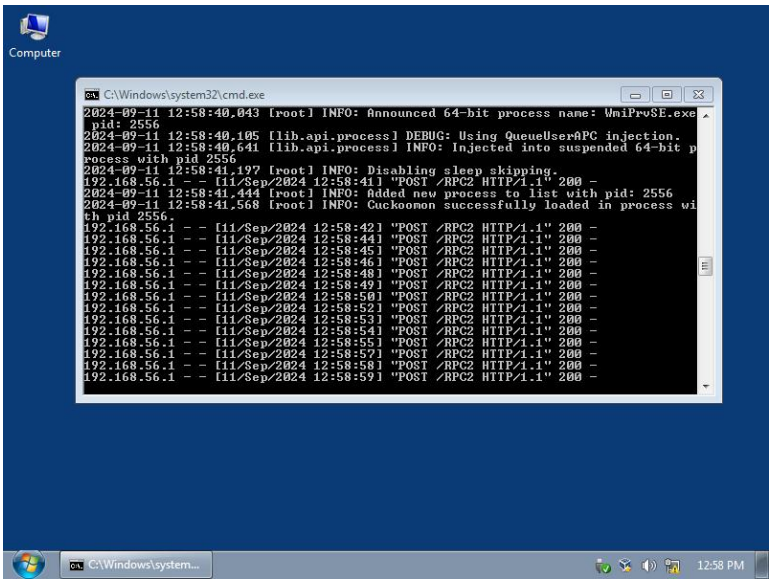

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:21,957 [root] INFO: Starting WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:22] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service is starting.192.168.56.1 - - [11/Sep/2024 12:58:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:25] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-09-11 12:58:25,766 [root] INFO: Started WMI Service
2024-09-11 12:58:25,766 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:26,178 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:26,247 [root] INFO: Added new process to list with pid: 2348
2024-09-11 12:58:26,247 [root] INFO: Cuckoomon successfully loaded in process with pid 2348.
2024-09-11 12:58:26,637 [root] INFO: Notified of termination of process with pid 2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

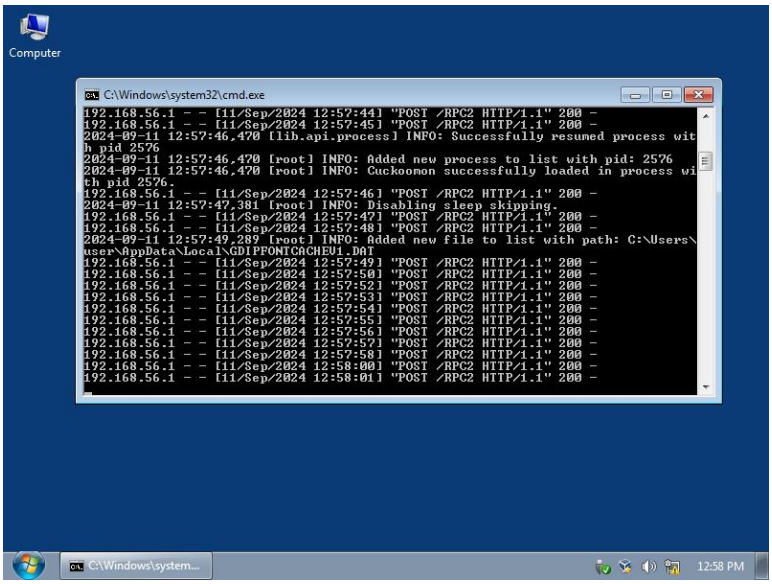

Computer
C:\Windows\system32\cmd.exe
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:17] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was stopped successfully.
2024-09-11 12:58:17,631 [root] INFO: Stopped WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:18] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-09-11 12:58:19,003 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:19,378 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:19,461 [root] INFO: Added new process to list with pid: 556
2024-09-11 12:58:19,461 [root] INFO: Cuckoomon successfully loaded in process with pid 556.
192.168.56.1 - - [11/Sep/2024 12:58:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:21] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:21,957 [root] INFO: Starting WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:22] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service is starting.192.168.56.1 - - [11/Sep/2024 12:58:23] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

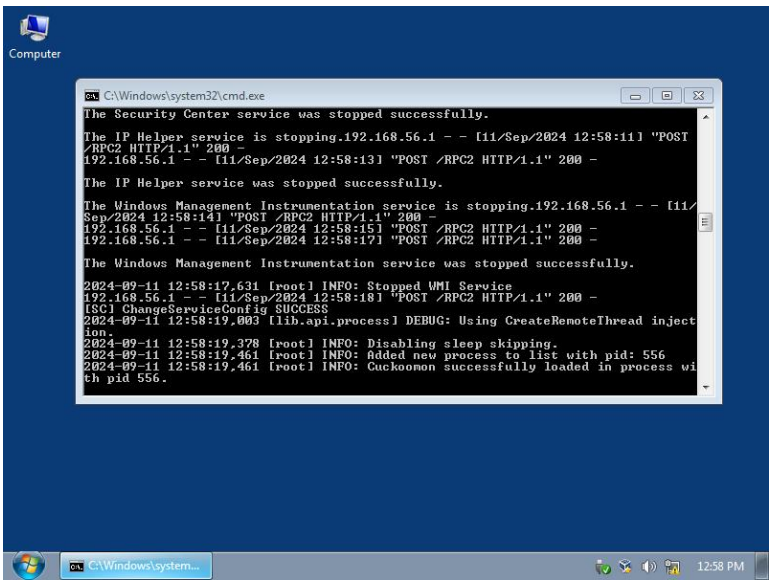

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Usage
2024-09-11 12:57:44,405 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\1d70518cc76abf62a24da3c74f1f349191ae702f.exe" with arguments "" with pid 2576
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process with pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process with pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:53] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:57 PM

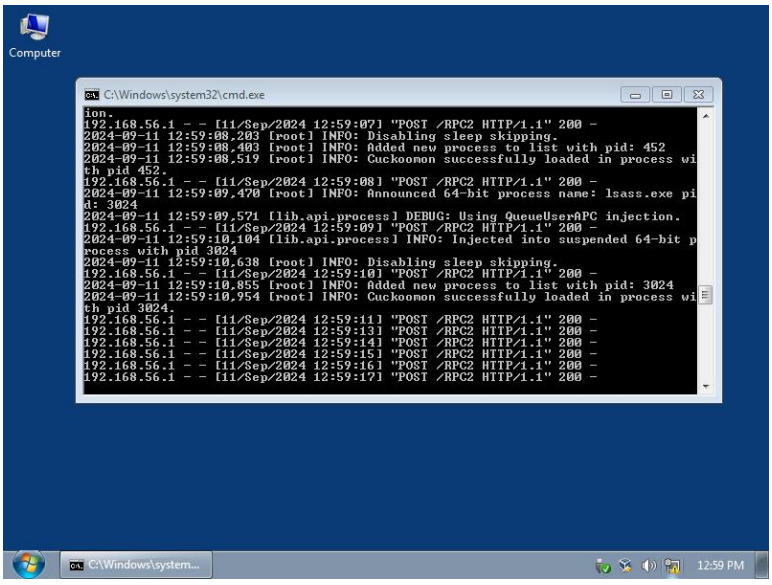

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:55] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

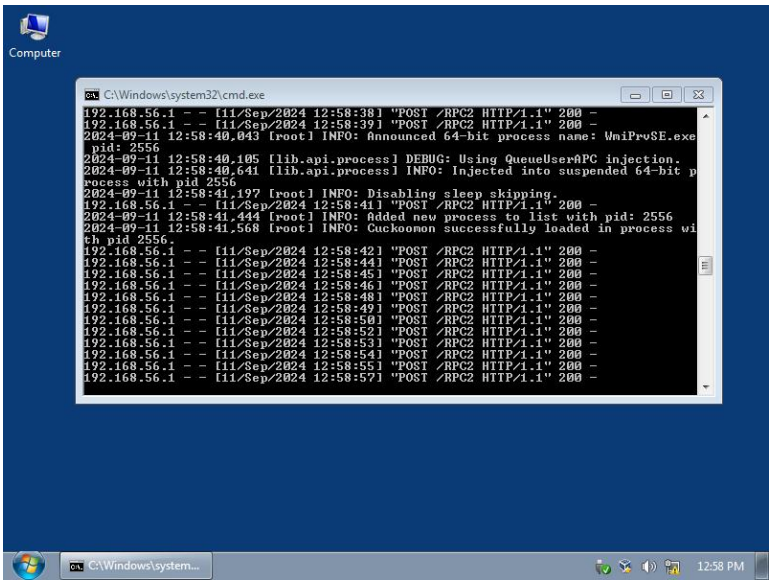

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:02] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

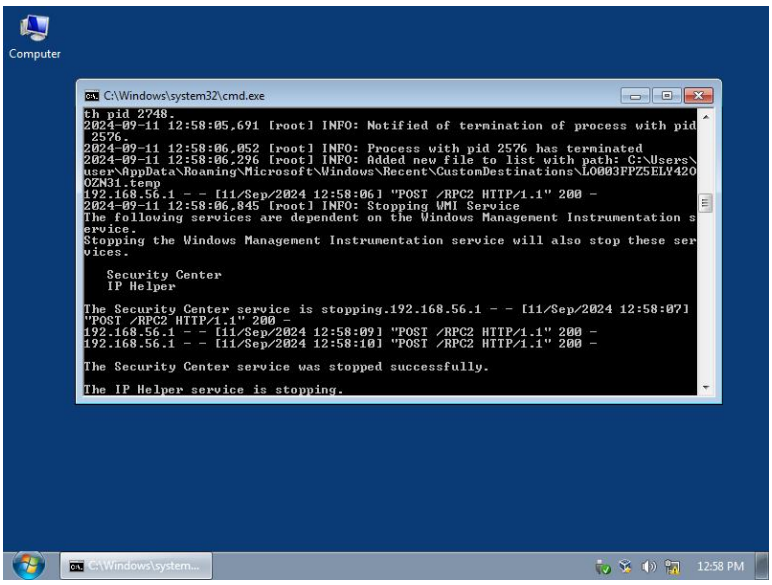

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:59] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

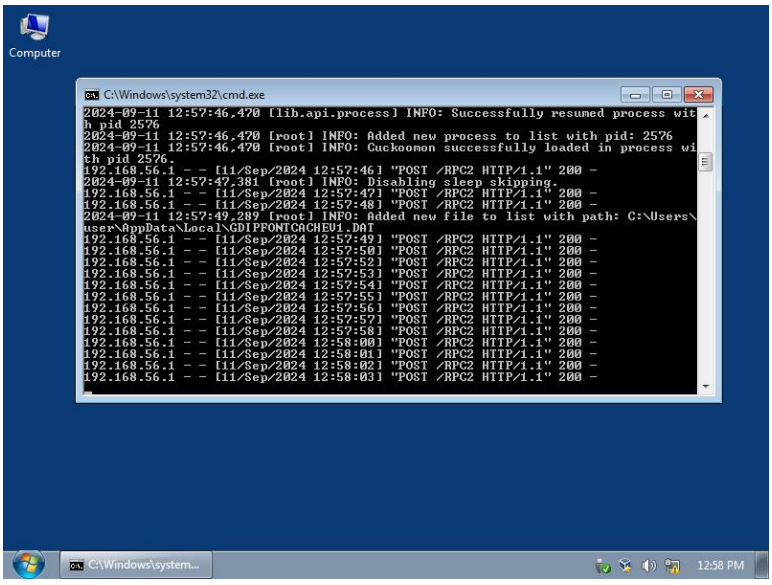

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process with pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process with pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\GDIFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:01] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

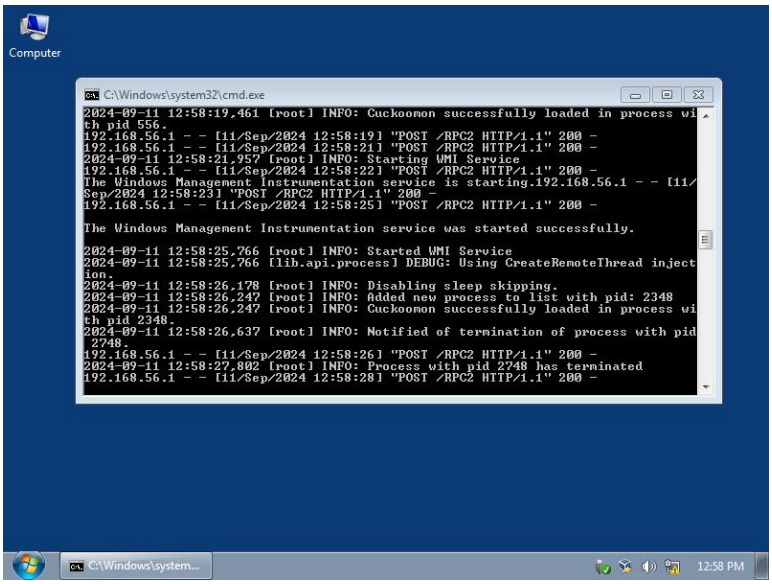

Computer
C:\Windows\system32\cmd.exe
The Security Center service was stopped successfully.
The IP Helper service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:13] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:17] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was stopped successfully.
2024-09-11 12:58:17,631 [root] INFO: Stopped WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:18] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-09-11 12:58:19,003 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:19,378 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:19,461 [root] INFO: Added new process to list with pid: 556
2024-09-11 12:58:19,461 [root] INFO: Cuckoomon successfully loaded in process with pid 556.
C:\Windows\system...
12:58 PM

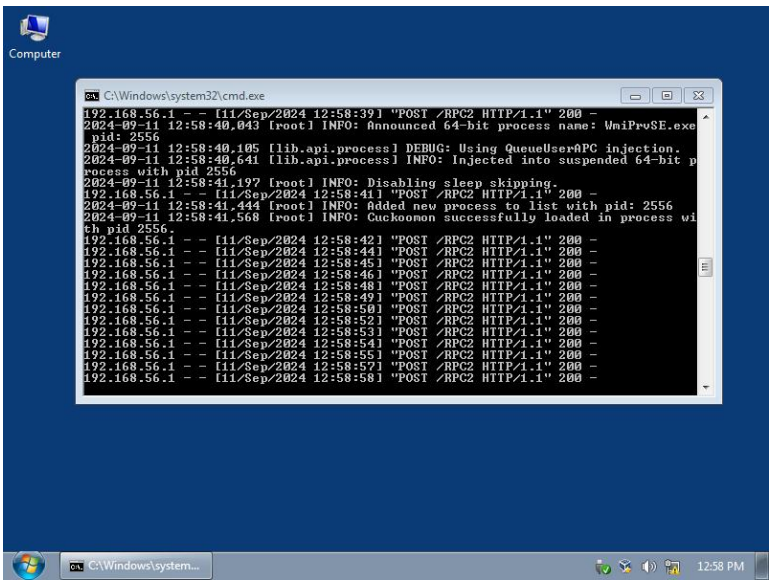

Computer
C:\Windows\system32\cmd.exe
ion.
192.168.56.1 - - [11/Sep/2024 12:59:07] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:08,203 [root] INFO: Disabling sleep skipping.
2024-09-11 12:59:08,403 [root] INFO: Added new process to list with pid: 452
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:17] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:59 PM

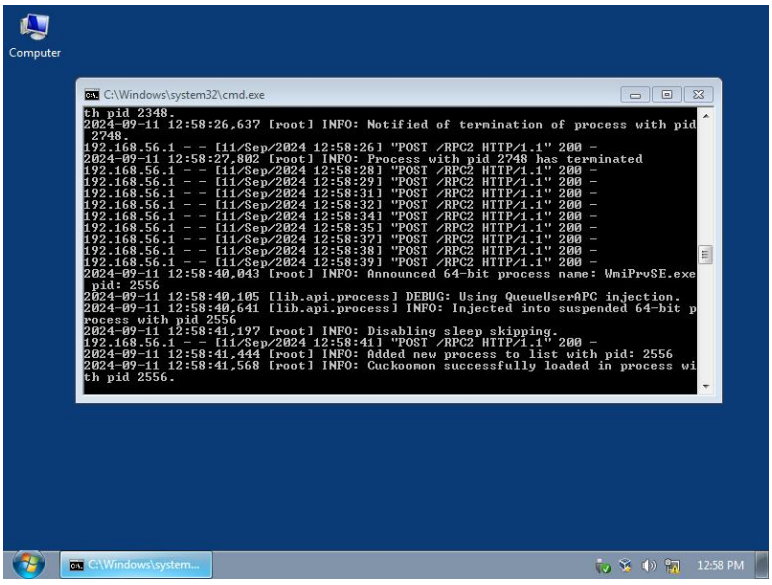

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe
pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:57] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

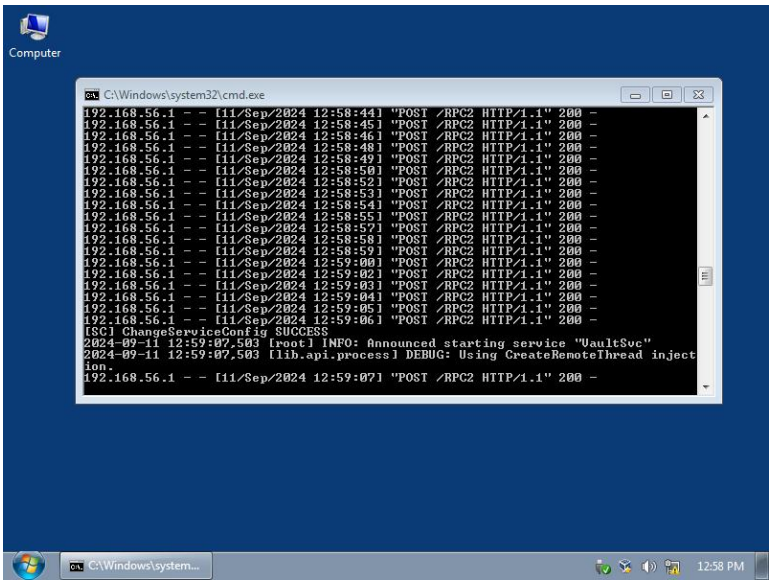

Computer
C:\Windows\system32\cmd.exe
th pid 2748.
2024-09-11 12:58:05,691 [root] INFO: Notified of termination of process with pid
2576.
2024-09-11 12:58:06,052 [root] INFO: Process with pid 2576 has terminated
2024-09-11 12:58:06,296 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\L0003FPZ5ELY420
OZN31.temp
192.168.56.1 - - [11/Sep/2024 12:58:06] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:06,845 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation s
ervice.
Stopping the Windows Management Instrumentation service will also stop these ser
vices.
Security Center
IP Helper
The Security Center service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:07]
"POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:10] "POST /RPC2 HTTP/1.1" 200 -
The Security Center service was stopped successfully.
The IP Helper service is stopping.
C:\Windows\system...
12:58 PM

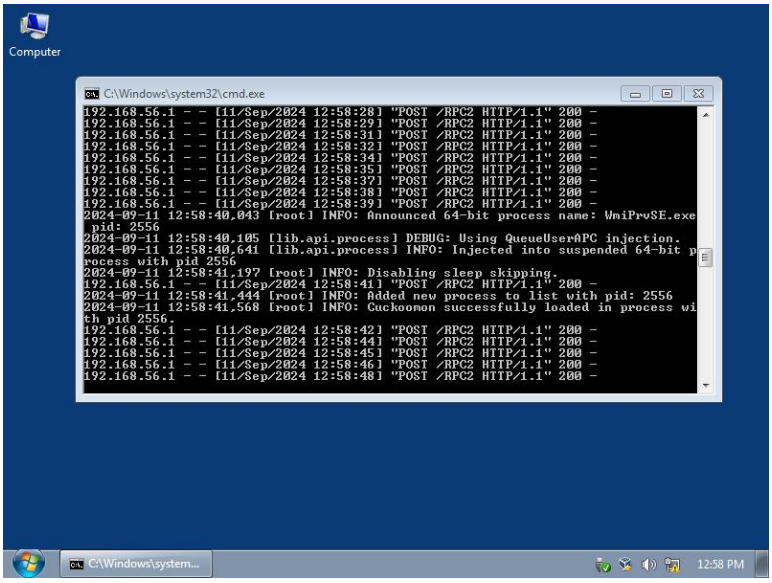

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process wit
h pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\GDIPFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:03] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

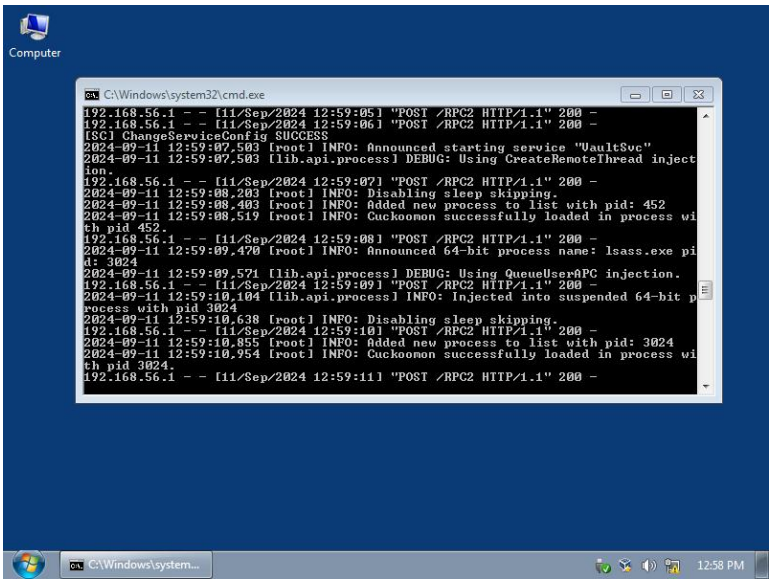

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:19,461 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 556.
192.168.56.1 - - [11/Sep/2024 12:58:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:21] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:21,957 [root] INFO: Starting WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:22] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service is starting.192.168.56.1 - - [11/
Sep/2024 12:58:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:25] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-09-11 12:58:25,766 [root] INFO: Started WMI Service
2024-09-11 12:58:25,766 [lib.api.process] DEBUG: Using CreateRemoteThread inject
ion.
2024-09-11 12:58:26,178 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:26,247 [root] INFO: Added new process to list with pid: 2348
2024-09-11 12:58:26,247 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2348.
2024-09-11 12:58:26,637 [root] INFO: Notified of termination of process with pid
2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

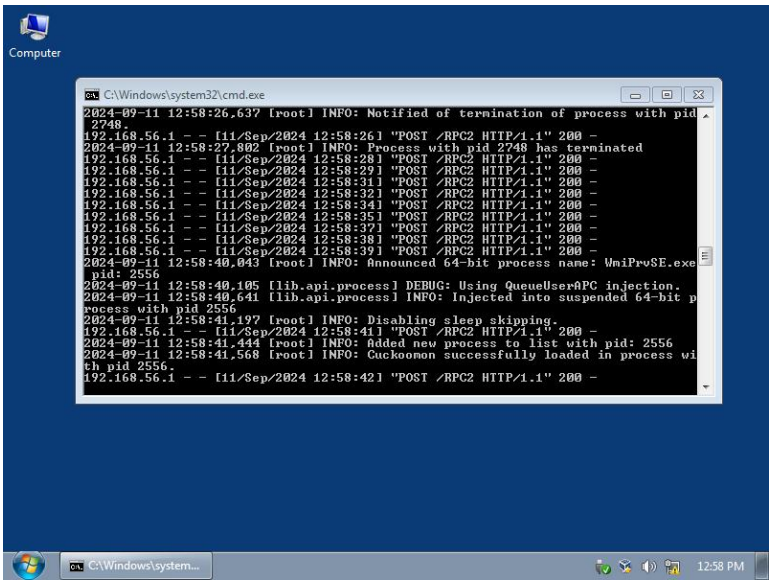

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe
pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:58] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

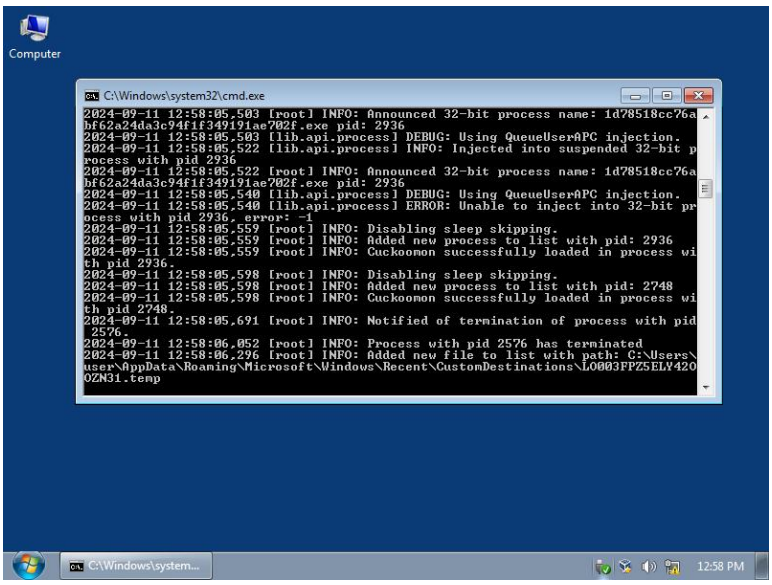

Computer
C:\Windows\system32\cmd.exe
th pid 2348.
2024-09-11 12:58:26,637 [root] INFO: Notified of termination of process with pid
2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe
pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2556.
C:\Windows\system...
12:58 PM

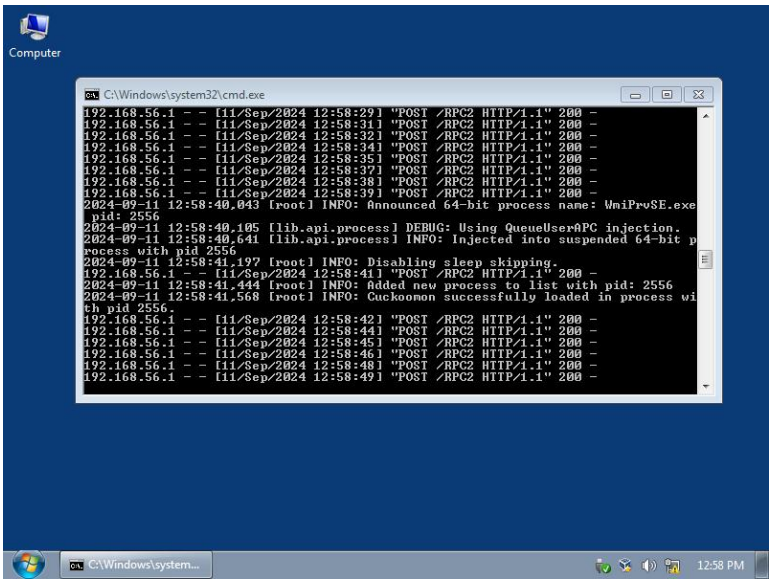

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:06] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-09-11 12:59:07,503 [root] INFO: Announced starting service "VaultSvc"
2024-09-11 12:59:07,503 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
192.168.56.1 - - [11/Sep/2024 12:59:07] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

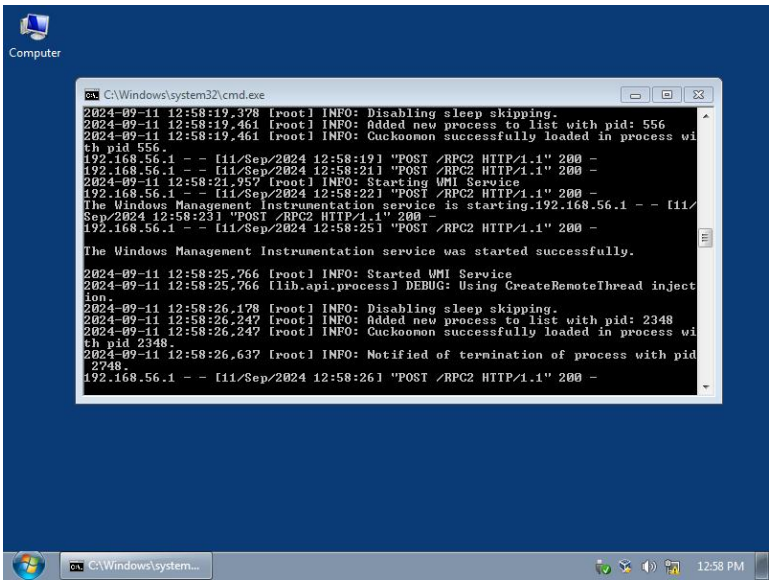

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

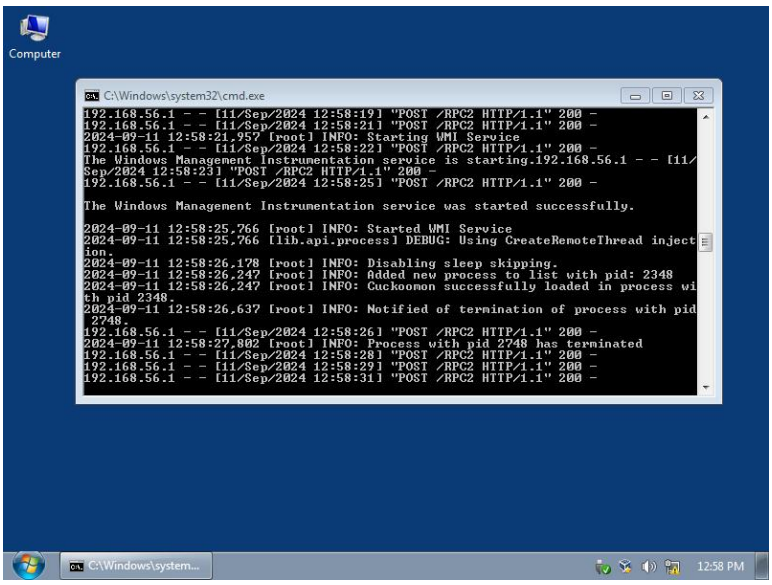

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:59:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:06] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-09-11 12:59:07,503 [root] INFO: Announced starting service "VaultSvc"
2024-09-11 12:59:07,503 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
192.168.56.1 - - [11/Sep/2024 12:59:07] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:08,203 [root] INFO: Disabling sleep skipping.
2024-09-11 12:59:08,403 [root] INFO: Added new process to list with pid: 452
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

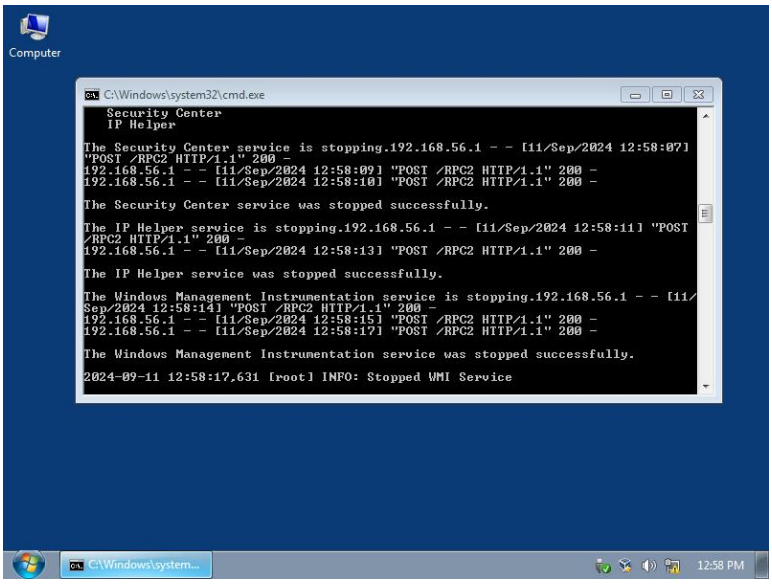

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:26,637 [root] INFO: Notified of termination of process with pid 2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

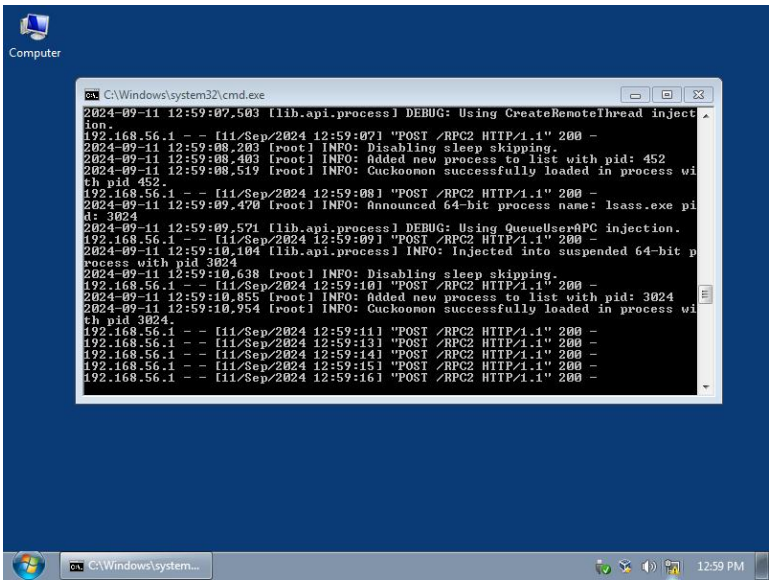

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:05,503 [root] INFO: Announced 32-bit process name: 1d78518cc76abf62a24da3c94f1f349191ae702f.exe pid: 2936
2024-09-11 12:58:05,503 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:05,522 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2936
2024-09-11 12:58:05,522 [root] INFO: Announced 32-bit process name: 1d78518cc76abf62a24da3c94f1f349191ae702f.exe pid: 2936
2024-09-11 12:58:05,540 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:05,540 [lib.api.process] ERROR: Unable to inject into 32-bit process with pid 2936, error: -1
2024-09-11 12:58:05,559 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:05,559 [root] INFO: Added new process to list with pid: 2936
2024-09-11 12:58:05,559 [root] INFO: Cuckoomon successfully loaded in process with pid 2936.
2024-09-11 12:58:05,598 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:05,598 [root] INFO: Added new process to list with pid: 2748
2024-09-11 12:58:05,598 [root] INFO: Cuckoomon successfully loaded in process with pid 2748.
2024-09-11 12:58:05,691 [root] INFO: Notified of termination of process with pid 2576.
2024-09-11 12:58:06,052 [root] INFO: Process with pid 2576 has terminated
2024-09-11 12:58:06,296 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\L0003FPZ5ELY420OZN31.temp
C:\Windows\system...
12:58 PM

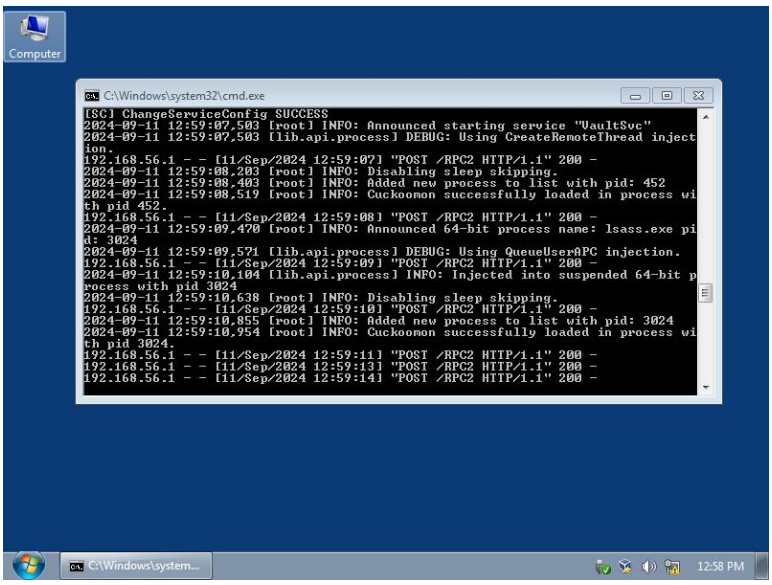

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

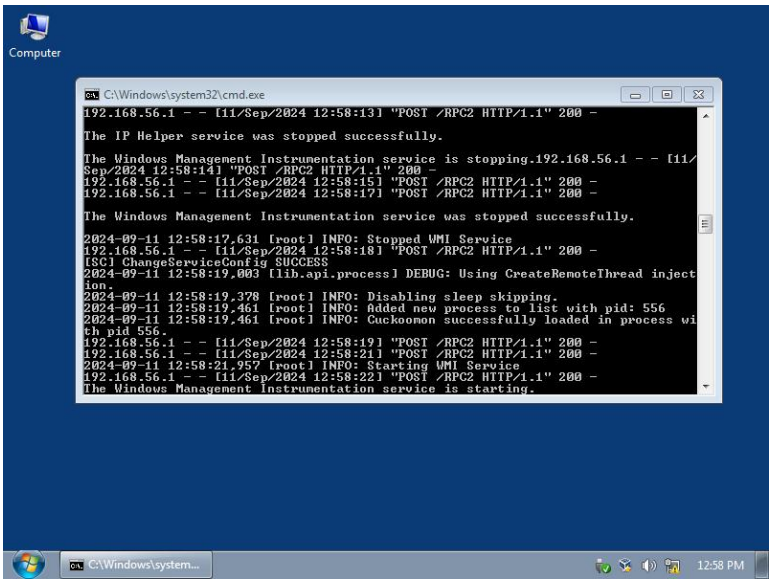

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:19,378 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:19,461 [root] INFO: Added new process to list with pid: 556
2024-09-11 12:58:19,461 [root] INFO: Cuckoomon successfully loaded in process with pid 556.
192.168.56.1 - - [11/Sep/2024 12:58:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:21] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:21,957 [root] INFO: Starting WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:22] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service is starting.192.168.56.1 - - [11/Sep/2024 12:58:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:25] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-09-11 12:58:25,766 [root] INFO: Started WMI Service
2024-09-11 12:58:25,766 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:26,178 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:26,247 [root] INFO: Added new process to list with pid: 2348
2024-09-11 12:58:26,247 [root] INFO: Cuckoomon successfully loaded in process with pid 2348.
2024-09-11 12:58:26,637 [root] INFO: Notified of termination of process with pid 2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

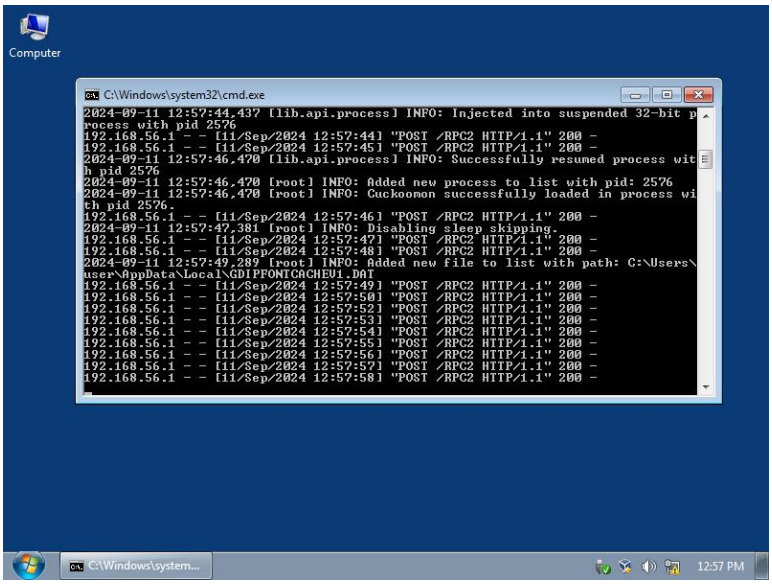

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:21] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:21,957 [root] INFO: Starting WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:22] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service is starting.192.168.56.1 - - [11/Sep/2024 12:58:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:25] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-09-11 12:58:25,766 [root] INFO: Started WMI Service
2024-09-11 12:58:25,766 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:26,178 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:26,247 [root] INFO: Added new process to list with pid: 2348
2024-09-11 12:58:26,247 [root] INFO: Cuckoomon successfully loaded in process with pid 2348.
2024-09-11 12:58:26,637 [root] INFO: Notified of termination of process with pid 2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

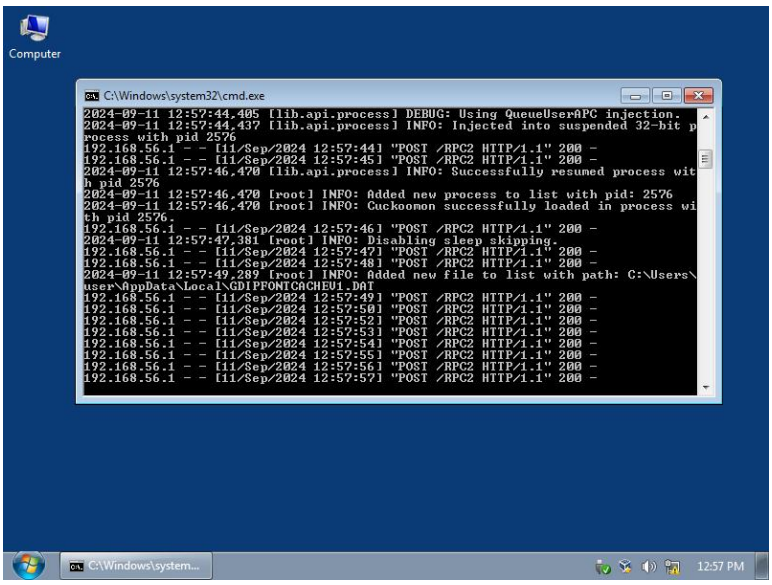

Computer
C:\Windows\system32\cmd.exe
Security Center
IP Helper
The Security Center service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:10] "POST /RPC2 HTTP/1.1" 200 -
The Security Center service was stopped successfully.
The IP Helper service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:13] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:17] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was stopped successfully.
2024-09-11 12:58:17,631 [root] INFO: Stopped WMI Service
C:\Windows\system...
12:58 PM

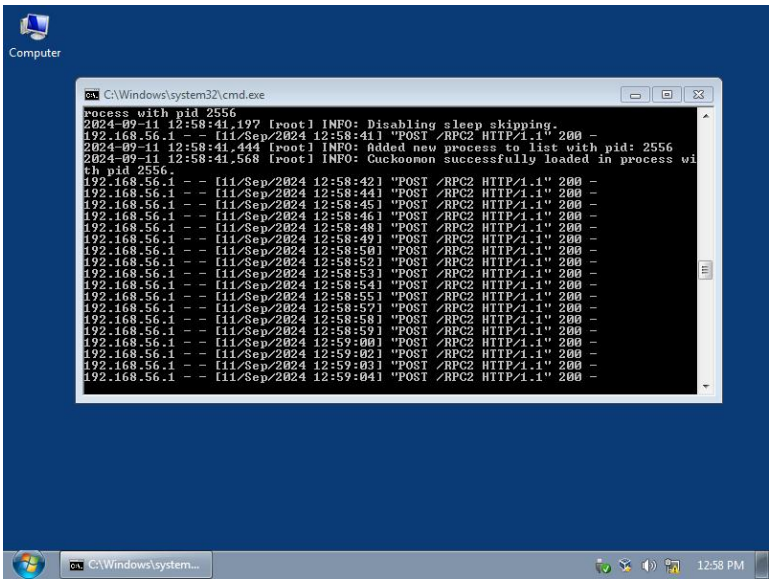

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:59:07,503 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
192.168.56.1 - - [11/Sep/2024 12:59:07] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:08,203 [root] INFO: Disabling sleep skipping.
2024-09-11 12:59:08,403 [root] INFO: Added new process to list with pid: 452
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:16] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:59 PM

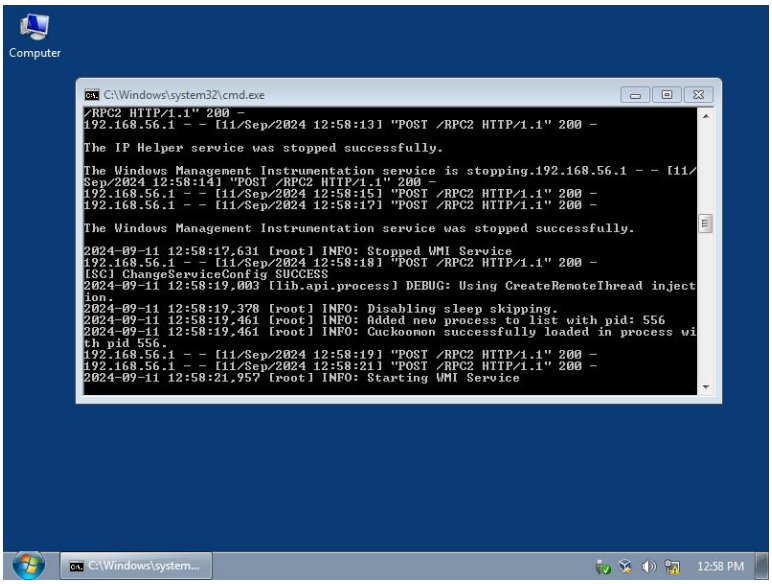

Computer
C:\Windows\system32\cmd.exe
[SC] ChangeServiceConfig SUCCESS
2024-09-11 12:59:07,503 [root] INFO: Announced starting service "Vault$vc"
2024-09-11 12:59:07,503 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
192.168.56.1 - - [11/Sep/2024 12:59:07] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:08,203 [root] INFO: Disabling sleep skipping.
2024-09-11 12:59:08,403 [root] INFO: Added new process to list with pid: 452
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:14] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

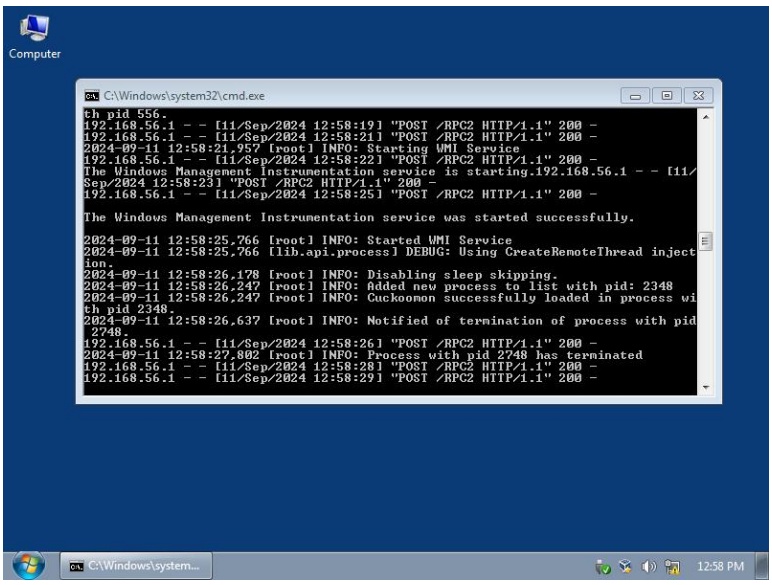

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:13] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:17] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was stopped successfully.
2024-09-11 12:58:17,631 [root] INFO: Stopped WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:18] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-09-11 12:58:19,003 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:19,378 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:19,461 [root] INFO: Added new process to list with pid: 556
2024-09-11 12:58:19,461 [root] INFO: Cuckoomon successfully loaded in process with pid 556.
192.168.56.1 - - [11/Sep/2024 12:58:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:21] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:21,957 [root] INFO: Starting WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:22] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service is starting.
C:\Windows\system...
12:58 PM

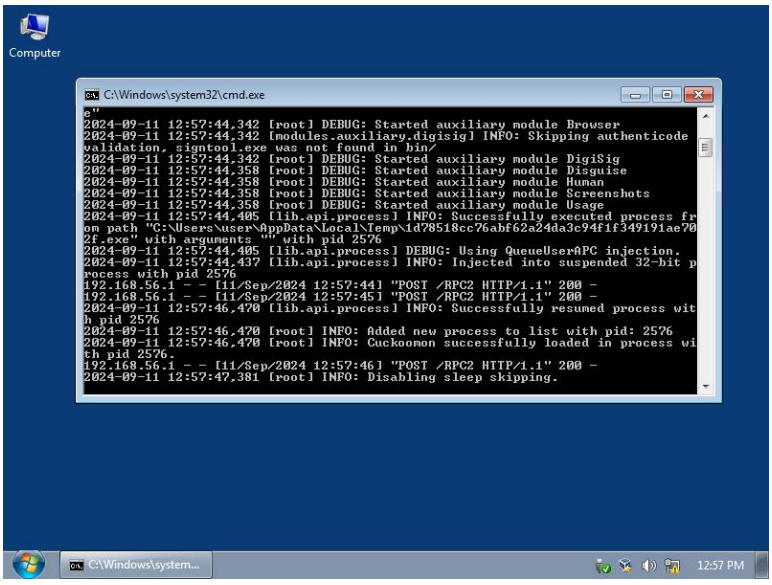

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process with pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process with pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:58] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:57 PM

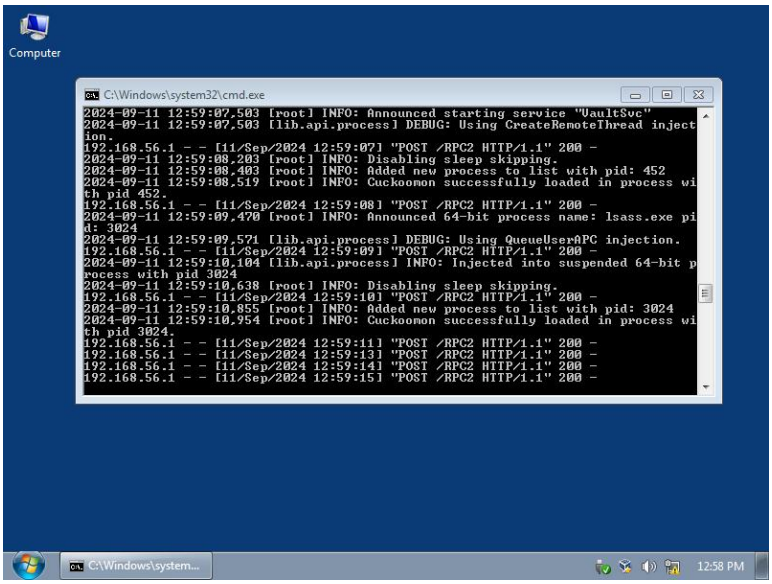

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process with pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process with pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:57] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:57 PM

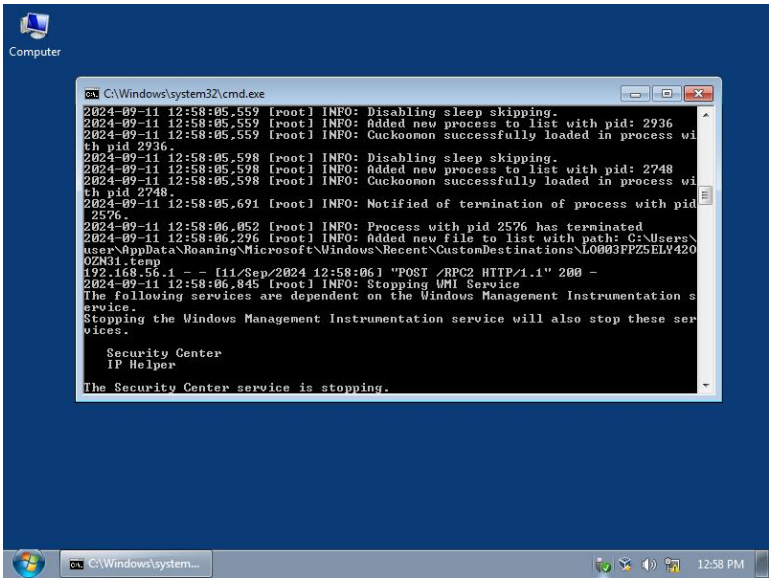

Computer
C:\Windows\system32\cmd.exe
rocess with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:04] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

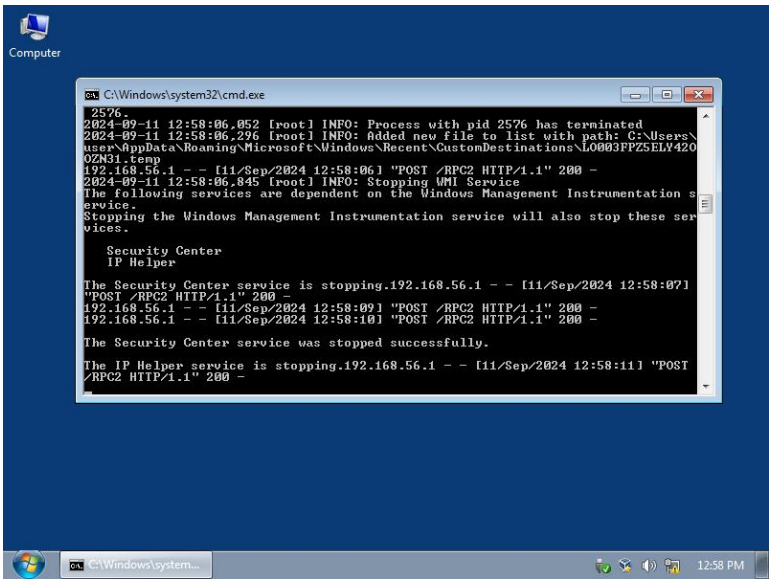

Computer
C:\Windows\system32\cmd.exe
/RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:13] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:17] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was stopped successfully.
2024-09-11 12:58:17,631 [root] INFO: Stopped WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:18] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-09-11 12:58:19,003 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:19,378 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:19,461 [root] INFO: Added new process to list with pid: 556
2024-09-11 12:58:19,461 [root] INFO: Cuckoomon successfully loaded in process with pid 556.
192.168.56.1 - - [11/Sep/2024 12:58:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:21] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:21,957 [root] INFO: Starting WMI Service
C:\Windows\system...
12:58 PM

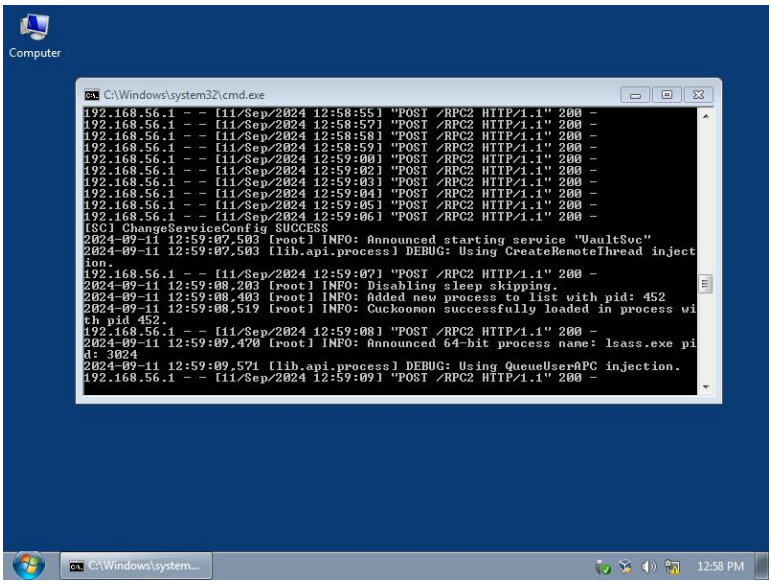

Computer
C:\Windows\system32\cmd.exe
th pid 556.
192.168.56.1 - - [11/Sep/2024 12:58:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:21] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:21,957 [root] INFO: Starting WMI Service
192.168.56.1 - - [11/Sep/2024 12:58:22] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service is starting.192.168.56.1 - - [11/Sep/2024 12:58:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:25] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-09-11 12:58:25,766 [root] INFO: Started WMI Service
2024-09-11 12:58:25,766 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:26,178 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:26,247 [root] INFO: Added new process to list with pid: 2348
2024-09-11 12:58:26,247 [root] INFO: Cuckoomon successfully loaded in process with pid 2348.
2024-09-11 12:58:26,637 [root] INFO: Notified of termination of process with pid 2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

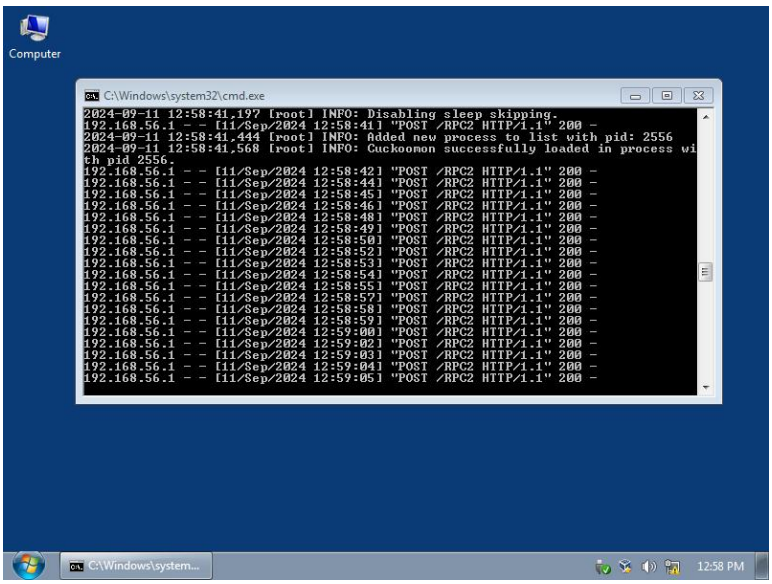

Computer
C:\Windows\system32\cmd.exe
e"
2024-09-11 12:57:44,342 [root] DEBUG: Started auxiliary module Browser
2024-09-11 12:57:44,342 [modules.auxiliary.digisig] INFO: Skipping authenticode validation, signtool.exe was not found in bin/
2024-09-11 12:57:44,342 [root] DEBUG: Started auxiliary module DigiSig
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Disguise
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Human
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Screenshots
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Usage
2024-09-11 12:57:44,405 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\1d78518cc76abf62a24da3c94f1f349191ae702f.exe" with arguments "" with pid 2576
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process with pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process with pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
C:\Windows\system...
12:57 PM

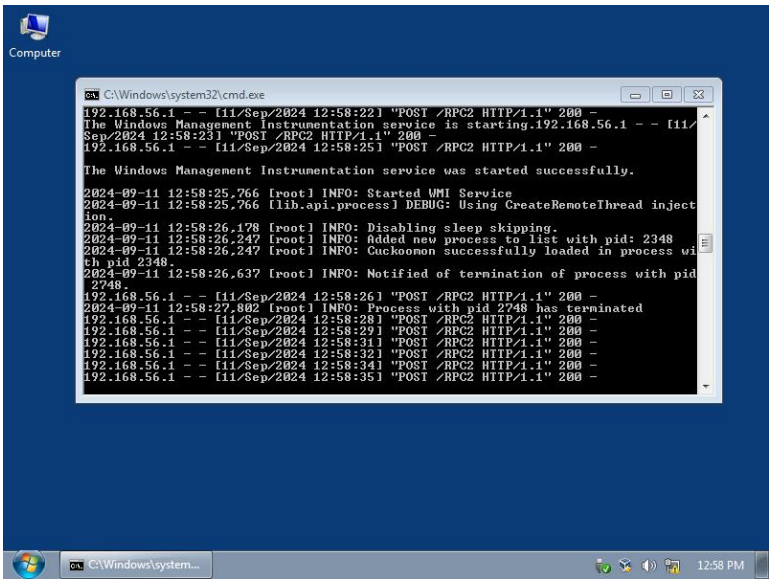

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:59:07,503 [root] INFO: Announced starting service "VaultSvc"
2024-09-11 12:59:07,503 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
192.168.56.1 - - [11/Sep/2024 12:59:07] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:08,203 [root] INFO: Disabling sleep skipping.
2024-09-11 12:59:08,403 [root] INFO: Added new process to list with pid: 452
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:15] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

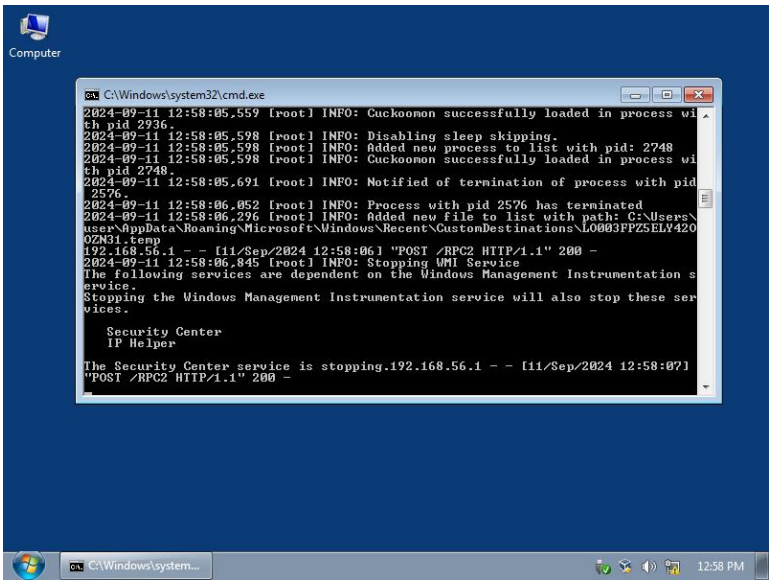

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:05,559 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:05,559 [root] INFO: Added new process to list with pid: 2936
2024-09-11 12:58:05,559 [root] INFO: Cuckoomon successfully loaded in process with pid 2936.
2024-09-11 12:58:05,598 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:05,598 [root] INFO: Added new process to list with pid: 2748
2024-09-11 12:58:05,598 [root] INFO: Cuckoomon successfully loaded in process with pid 2748.
2024-09-11 12:58:05,691 [root] INFO: Notified of termination of process with pid 2576.
2024-09-11 12:58:06,052 [root] INFO: Process with pid 2576 has terminated
2024-09-11 12:58:06,296 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\LO003FPZ5ELY420OZN31.temp
192.168.56.1 - - [11/Sep/2024 12:58:06] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:06,845 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.
Security Center
IP Helper
The Security Center service is stopping.
C:\Windows\system...
12:58 PM

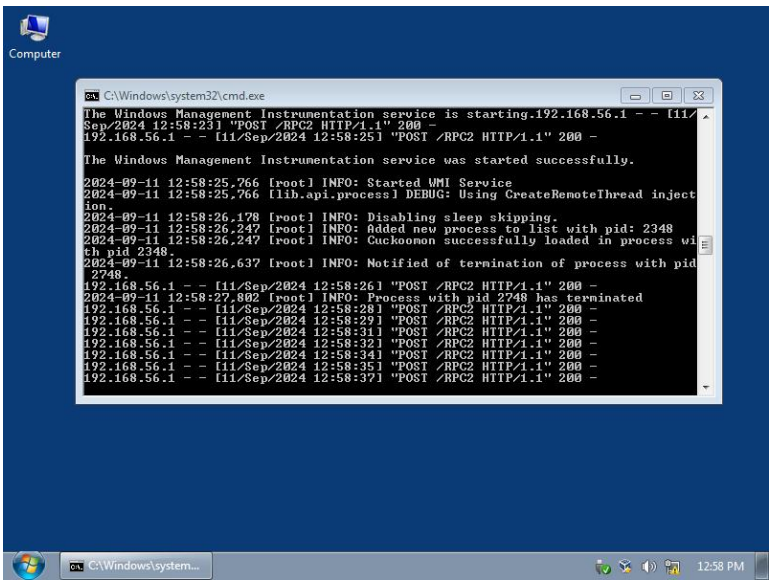

Computer
C:\Windows\system32\cmd.exe
2576.
2024-09-11 12:58:06,052 [root] INFO: Process with pid 2576 has terminated
2024-09-11 12:58:06,296 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\LO003FPZ5ELY420OZN31.temp
192.168.56.1 - - [11/Sep/2024 12:58:06] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:06,845 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.
Security Center
IP Helper
The Security Center service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:10] "POST /RPC2 HTTP/1.1" 200 -
The Security Center service was stopped successfully.
The IP Helper service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:11] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

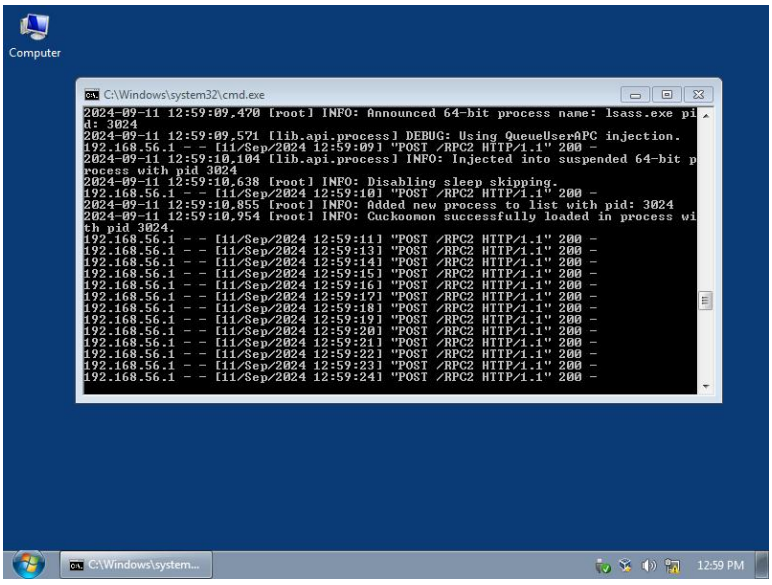

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:06] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-09-11 12:59:07,503 [root] INFO: Announced starting service "VaultSvc"
2024-09-11 12:59:07,503 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
192.168.56.1 - - [11/Sep/2024 12:59:07] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:08,203 [root] INFO: Disabling sleep skipping.
2024-09-11 12:59:08,403 [root] INFO: Added new process to list with pid: 452
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

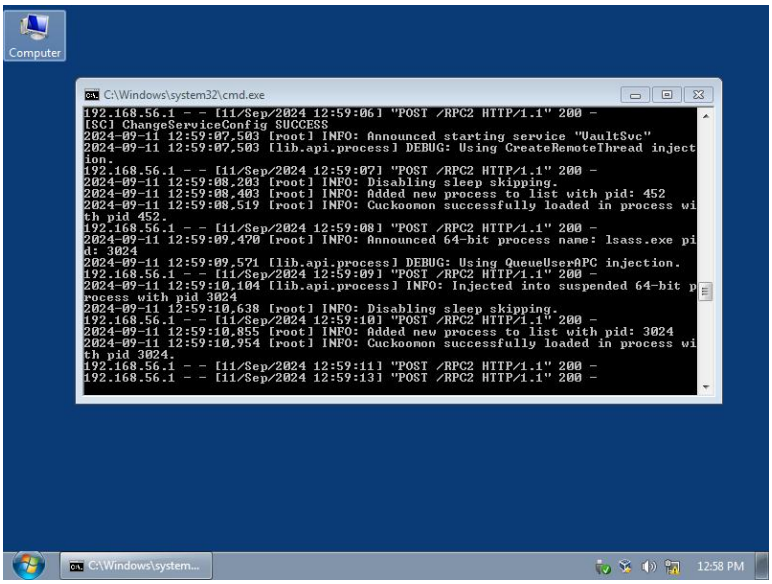

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:05] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

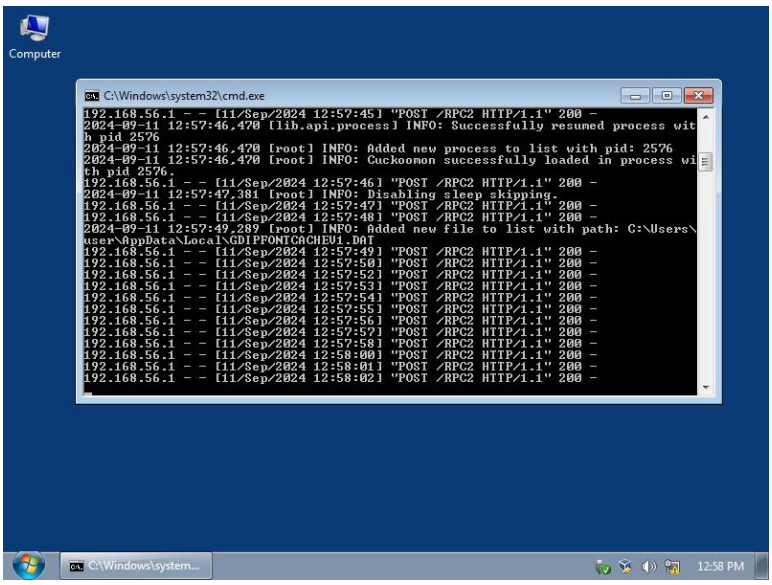

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:22] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service is starting.192.168.56.1 - - [11/Sep/2024 12:58:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:25] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-09-11 12:58:25,766 [root] INFO: Started WMI Service
2024-09-11 12:58:25,766 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:26,178 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:26,247 [root] INFO: Added new process to list with pid: 2348
2024-09-11 12:58:26,247 [root] INFO: Cuckoomon successfully loaded in process with pid 2348.
2024-09-11 12:58:26,637 [root] INFO: Notified of termination of process with pid 2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

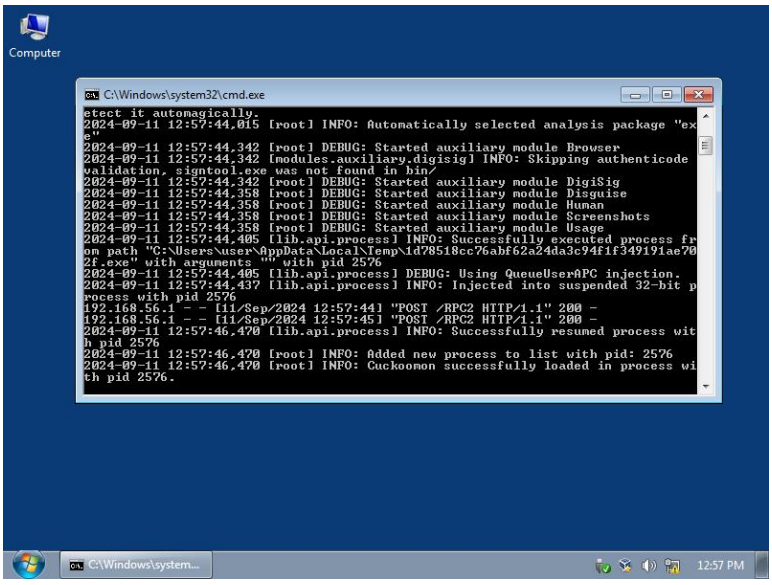

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:58:05,559 [root] INFO: Cuckoomon successfully loaded in process with pid 2936.
2024-09-11 12:58:05,598 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:05,598 [root] INFO: Added new process to list with pid: 2748
2024-09-11 12:58:05,598 [root] INFO: Cuckoomon successfully loaded in process with pid 2748.
2024-09-11 12:58:05,691 [root] INFO: Notified of termination of process with pid 2576.
2024-09-11 12:58:06,052 [root] INFO: Process with pid 2576 has terminated
2024-09-11 12:58:06,296 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\LO003FPZ5ELY420OZN31.temp
192.168.56.1 - - [11/Sep/2024 12:58:06] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:06,845 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.
Security Center
IP Helper
The Security Center service is stopping.192.168.56.1 - - [11/Sep/2024 12:58:07] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

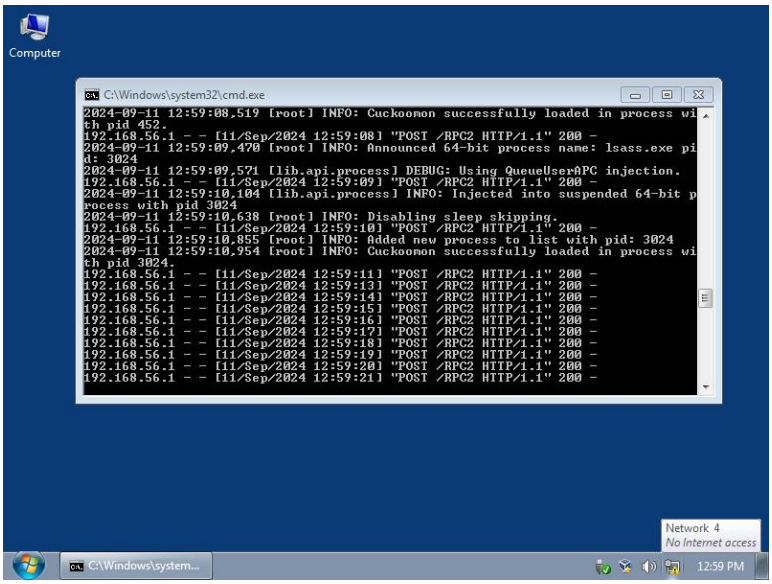

Computer
C:\Windows\system32\cmd.exe
The Windows Management Instrumentation service is starting.192.168.56.1 - - [11/Sep/2024 12:58:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:25] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-09-11 12:58:25,766 [root] INFO: Started WMI Service
2024-09-11 12:58:25,766 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-09-11 12:58:26,178 [root] INFO: Disabling sleep skipping.
2024-09-11 12:58:26,247 [root] INFO: Added new process to list with pid: 2348
2024-09-11 12:58:26,247 [root] INFO: Cuckoomon successfully loaded in process with pid 2348.
2024-09-11 12:58:26,637 [root] INFO: Notified of termination of process with pid 2748.
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

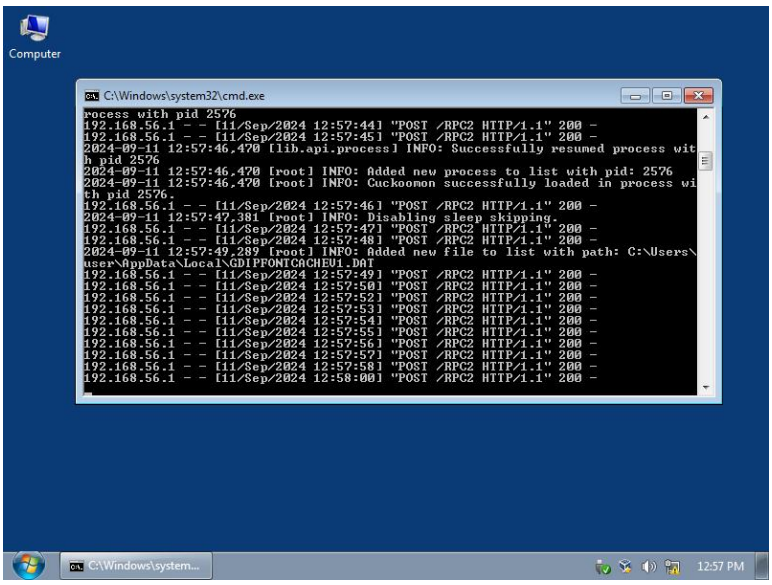

Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:24] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:59 PM

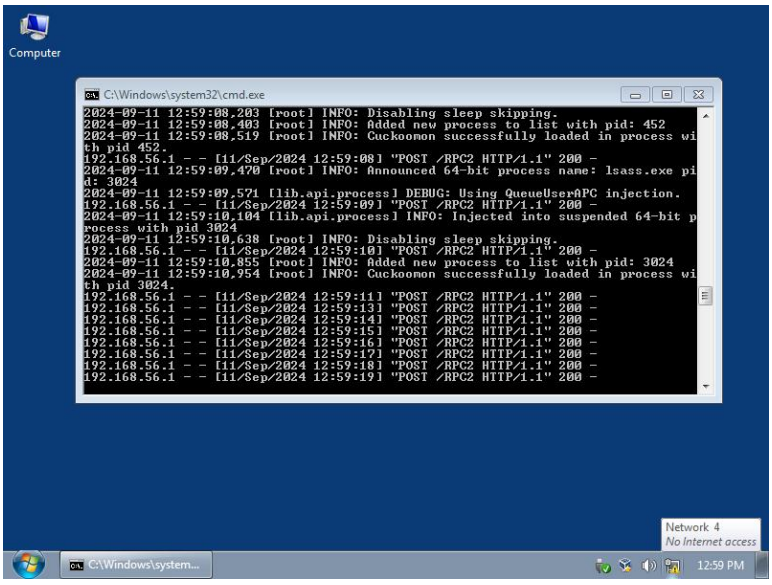

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:59:06] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-09-11 12:59:07,503 [root] INFO: Announced starting service "VaultSvc"
2024-09-11 12:59:07,503 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
192.168.56.1 - - [11/Sep/2024 12:59:07] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:08,203 [root] INFO: Disabling sleep skipping.
2024-09-11 12:59:08,403 [root] INFO: Added new process to list with pid: 452
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

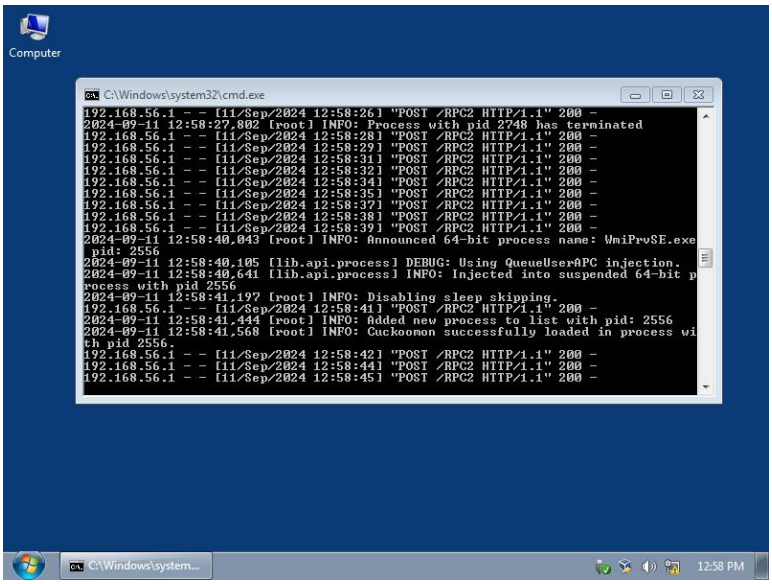

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process with pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process with pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:02] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM

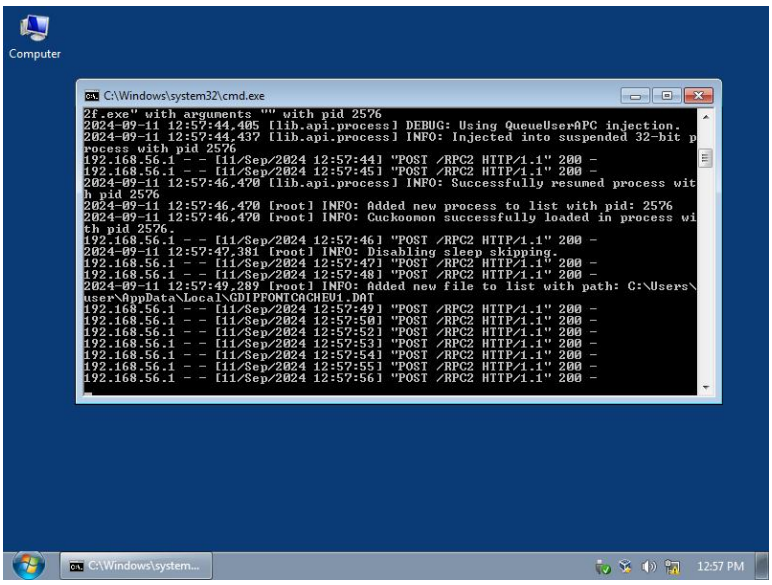

Computer
C:\Windows\system32\cmd.exe
etect it automagically.
2024-09-11 12:57:44,015 [root] INFO: Automatically selected analysis package "exe"
2024-09-11 12:57:44,342 [root] DEBUG: Started auxiliary module Browser
2024-09-11 12:57:44,342 [modules.auxiliary.digisig] INFO: Skipping authenticode validation, signtool.exe was not found in bin/
2024-09-11 12:57:44,342 [root] DEBUG: Started auxiliary module DigiSig
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Disguise
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Human
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Screenshots
2024-09-11 12:57:44,358 [root] DEBUG: Started auxiliary module Usage
2024-09-11 12:57:44,405 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\id70518cc76abf62a24da3c94f1f349191ae702f.exe" with arguments "" with pid 2576
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process with pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process with pid 2576.
C:\Windows\system...
12:57 PM


Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:21] "POST /RPC2 HTTP/1.1" 200 -
Network 4
No Internet access
C:\Windows\system...
12:59 PM


Computer
C:\Windows\system32\cmd.exe
process with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process with pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process with pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:00] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:57 PM


Computer
C:\Windows\system32\cmd.exe
2024-09-11 12:59:08,203 [root] INFO: Disabling sleep skipping.
2024-09-11 12:59:08,403 [root] INFO: Added new process to list with pid: 452
2024-09-11 12:59:08,519 [root] INFO: Cuckoomon successfully loaded in process with pid 452.
192.168.56.1 - - [11/Sep/2024 12:59:08] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:09,470 [root] INFO: Announced 64-bit process name: lsass.exe pid: 3024
2024-09-11 12:59:09,571 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [11/Sep/2024 12:59:09] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,104 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 3024
2024-09-11 12:59:10,638 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:59:10] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:59:10,855 [root] INFO: Added new process to list with pid: 3024
2024-09-11 12:59:10,954 [root] INFO: Cuckoomon successfully loaded in process with pid 3024.
192.168.56.1 - - [11/Sep/2024 12:59:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:59:19] "POST /RPC2 HTTP/1.1" 200 -
Network 4
No Internet access
C:\Windows\system...
12:59 PM


Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [11/Sep/2024 12:58:26] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:27,802 [root] INFO: Process with pid 2748 has terminated
192.168.56.1 - - [11/Sep/2024 12:58:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:39] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:40,043 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2556
2024-09-11 12:58:40,105 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:58:40,641 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2556
2024-09-11 12:58:41,197 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:58:41] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:58:41,444 [root] INFO: Added new process to list with pid: 2556
2024-09-11 12:58:41,568 [root] INFO: Cuckoomon successfully loaded in process with pid 2556.
192.168.56.1 - - [11/Sep/2024 12:58:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:58:45] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:58 PM


Computer
C:\Windows\system32\cmd.exe
2f.exe" with arguments "" with pid 2576
2024-09-11 12:57:44,405 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-09-11 12:57:44,437 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2576
192.168.56.1 - - [11/Sep/2024 12:57:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:45] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:46,470 [lib.api.process] INFO: Successfully resumed process with pid 2576
2024-09-11 12:57:46,470 [root] INFO: Added new process to list with pid: 2576
2024-09-11 12:57:46,470 [root] INFO: Cuckoomon successfully loaded in process with pid 2576.
192.168.56.1 - - [11/Sep/2024 12:57:46] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:47,381 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [11/Sep/2024 12:57:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:48] "POST /RPC2 HTTP/1.1" 200 -
2024-09-11 12:57:49,289 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT
192.168.56.1 - - [11/Sep/2024 12:57:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [11/Sep/2024 12:57:56] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:57 PM