VALKYRIE COMODO

Summary

File Name: virussign.com_0294f103cf2a4bf978983b54ee882ee6.exe

File Type: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows

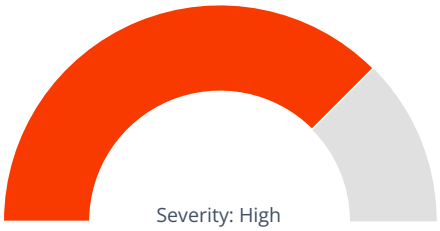
SHA1: 019c6ae7809e3c860a8d93eea365de57d128b6b9

MD5: 0294f103cf2a4bf978983b54ee882ee6

MALWARE

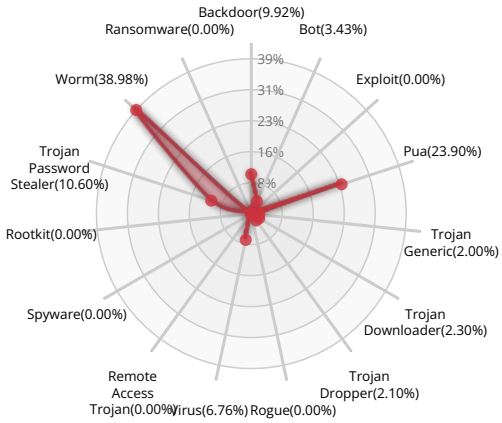
Valkyrie Final Verdict

DETECTION SECTION

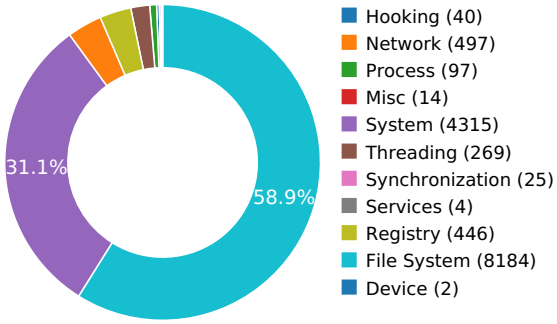


Verdict: Malware

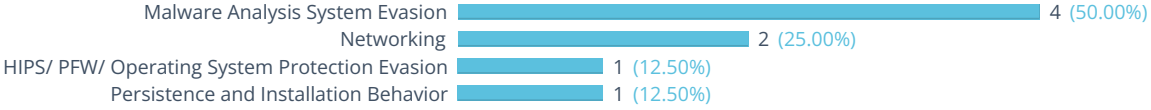
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

NETWORKING

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

Starts servers listening on 0.0.0.0:3159

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Attempts to identify installed AV products by installation directory Show sources

MALWARE ANALYSIS SYSTEM EVASION

Checks the presence of disk drives in the registry, possibly for anti-virtualization Show sources

Attempts to identify installed analysis tools by a known file location Show sources

A process attempted to delay the analysis task by a long amount of time. Show sources

Creates a hidden or system file Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup Show sources

Behavior Graph

21:19:10 **21:20:48** **21:22:27**

PID 2300

21:19:10 **Create Process** The malicious file created a child process as 019c6ae7809e3c860a8d93eea365de57d128b6b9.exe **(PPID 2244)**

21:19:10 RegQueryValueExA

21:19:10 NtDelayExecution

21:19:10 NtSetInformationFile

21:19:14 Create Process

PID 2468

21:19:14 **Create Process** The malicious file created a child process as ctfmen.exe **(PPID 2300)**

21:19:15 Create Process

PID 2536

21:19:15 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2468)**

21:19:15 NtDelayExecution

21:19:28 Create Process

PID 2760

21:19:29 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2536)**

21:19:31 RegSetValueExA

21:19:42 Create Process

21:19:46 21:20:29 WSAConnect **[4 times]**

21:19:52 Create Process

21:20:02 Create Process

21:20:12 Create Process

21:20:23 Create Process

21:20:33 Create Process

21:20:36 21:20:36 FindFirstFileExW **[2 times]**

21:20:36 21:20:36 NtCreateFile **[12 times]**

21:20:43 WSAConnect

21:20:43 Create Process

21:20:43 FindFirstFileExW

21:20:53 Create Process

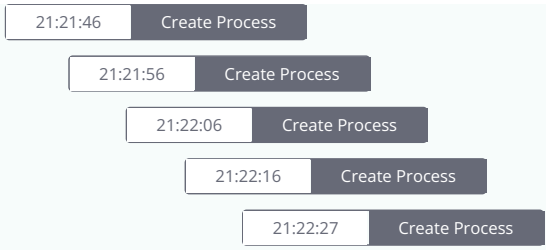
21:20:57 21:22:23 WSAConnect **[7 times]**

21:21:04 Create Process

21:21:15 Create Process

21:21:25 Create Process

21:21:35 Create Process



PID 2960

21:19:45 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 1988

21:19:59 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 2076

21:20:13 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 2312

21:20:26 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 2620

21:20:38 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 792

21:20:48 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 2612

21:20:58 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 3020

21:21:06 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 2172

21:21:14 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 2420

21:21:22 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 1308

21:21:28 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 780

21:21:36 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 2752

21:21:44 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 1684

21:21:53 **Create Process** The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 820

21:22:03 | Create Process | The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 540

21:22:14 | Create Process | The malicious file created a child process as smnss.exe **(PPID 2760)**

PID 3016

21:22:26 | Create Process | The malicious file created a child process as smnss.exe **(PPID 2760)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\System32\ctfmen.exe
C:\Windows\System32\tzres.dll
C:\Program Files\Common Files\System\symsrv.dll
C:\Users\user\AppData\Local\Temp\A1D26E2
C:\Windows\System32\user32.dll
C:\Windows\System32\shervans.dll
C:\Users\user\AppData\Local\Temp\019c6ae7809e3c860a8d93eea365de57d128b6b9.exe
C:\Windows\System32\grcopy.dll
C:\Windows\System32\smnss.exe
C:\Windows\System32\satornas.dll
C:\Program Files\Common Files\System\symsrv.dll.dat
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\zipfi.dll
C:\Windows\System32\zipfiaq.dll
\Device\KsecDD
C:*.*
C:\$Recycle.Bin*.*
C:\$Recycle.Bin\S-1-5-21-2298303332-66077612-2598613238-1000*.*
C:\CXNLWFFzvR*.*
C:\CXNLWFFzvR\drop*.*
C:\CXNLWFFzvR\files*.*
C:\CXNLWFFzvR\logs*.*
C:\CXNLWFFzvR\memory*.*
C:\CXNLWFFzvR\shots*.*
C:\Documents and Settings*.*
C:\fTuLvth*.*
C:\fTuLvth\drop*.*
C:\fTuLvth\files*.*
C:\fTuLvth\logs*.*
C:\fTuLvth\memory*.*
C:\fTuLvth\shots*.*
C:\nidguu*.*

C:\nidguu\bin*.*
C:\nidguu\dll*.*
C:\nidguu\lib*.*
C:\nidguu\lib\api*.*
C:\nidguu\lib\common*.*
C:\nidguu\lib\core*.*
C:\nidguu\modules*.*
C:\nidguu\modules\auxiliary*.*
C:\nidguu\modules\packages*.*
C:\Program Files*.*
C:\Program Files\7-Zip*.*
C:\Program Files\7-Zip\History.txt
C:\Program Files\7-Zip\Lang*.*
C:\Program Files\7-Zip\Lang\af.txt
C:\Program Files\7-Zip\Lang\an.txt
C:\Program Files\7-Zip\Lang\ar.txt
C:\Program Files\7-Zip\Lang\ast.txt
C:\Program Files\7-Zip\Lang\az.txt
C:\Program Files\7-Zip\Lang\ba.txt
C:\Program Files\7-Zip\Lang\be.txt
C:\Program Files\7-Zip\Lang\bg.txt
C:\Program Files\7-Zip\Lang\bn.txt
C:\Program Files\7-Zip\Lang\br.txt
C:\Program Files\7-Zip\Lang\ca.txt
C:\Program Files\7-Zip\Lang\co.txt
C:\Program Files\7-Zip\Lang\cs.txt
C:\Program Files\7-Zip\Lang\cy.txt
C:\Program Files\7-Zip\Lang\da.txt
C:\Program Files\7-Zip\Lang\de.txt
C:\Program Files\7-Zip\Lang\el.txt
C:\Program Files\7-Zip\Lang\eo.txt
C:\Program Files\7-Zip\Lang\es.txt
C:\Program Files\7-Zip\Lang\et.txt
C:\Program Files\7-Zip\Lang\eu.txt
C:\Program Files\7-Zip\Lang\ext.txt

C:\Program Files\7-Zip\Lang\fa.txt
C:\Program Files\7-Zip\Lang\fi.txt
C:\Program Files\7-Zip\Lang\fr.txt
C:\Program Files\7-Zip\Lang\fur.txt
C:\Program Files\7-Zip\Lang\fy.txt
C:\Program Files\7-Zip\Lang\ga.txt
C:\Program Files\7-Zip\Lang\gl.txt
C:\Program Files\7-Zip\Lang\gu.txt
C:\Program Files\7-Zip\Lang\he.txt

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\0
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\1
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\usw
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\pafw
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\usbactiv
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\namecp
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\statem
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\time
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\iduser

MODIFIED FILES

C:\Windows\System32\ctfmen.exe
C:\Windows\System32\shervans.dll
C:\Windows\System32\grcopy.dll
C:\Windows\System32\smnss.exe
C:\Windows\System32\satornas.dll
C:\Windows\System32\zipfi.dll
C:\Windows\System32\zipfiaq.dll

C:\Program Files\7-Zip\History.txt

C:\Program Files\7-Zip\Lang\af.txt

C:\Program Files\7-Zip\Lang\an.txt

C:\Program Files\7-Zip\Lang\ar.txt

C:\Program Files\7-Zip\Lang\ast.txt

C:\Program Files\7-Zip\Lang\az.txt

C:\Program Files\7-Zip\Lang\ba.txt

C:\Program Files\7-Zip\Lang\be.txt

C:\Program Files\7-Zip\Lang\bg.txt

C:\Program Files\7-Zip\Lang\bn.txt

C:\Program Files\7-Zip\Lang\br.txt

C:\Program Files\7-Zip\Lang\ca.txt

C:\Program Files\7-Zip\Lang\co.txt

C:\Program Files\7-Zip\Lang\cs.txt

C:\Program Files\7-Zip\Lang\cy.txt

C:\Program Files\7-Zip\Lang\da.txt

C:\Program Files\7-Zip\Lang\de.txt

C:\Program Files\7-Zip\Lang\el.txt

C:\Program Files\7-Zip\Lang\eo.txt

C:\Program Files\7-Zip\Lang\es.txt

C:\Program Files\7-Zip\Lang\et.txt

C:\Program Files\7-Zip\Lang\eu.txt

C:\Program Files\7-Zip\Lang\ext.txt

C:\Program Files\7-Zip\Lang\fa.txt

C:\Program Files\7-Zip\Lang\fi.txt

C:\Program Files\7-Zip\Lang\fr.txt

C:\Program Files\7-Zip\Lang\fur.txt

C:\Program Files\7-Zip\Lang\fy.txt

C:\Program Files\7-Zip\Lang\ga.txt

C:\Program Files\7-Zip\Lang\gl.txt

C:\Program Files\7-Zip\Lang\gu.txt

C:\Program Files\7-Zip\Lang\he.txt

C:\Program Files\7-Zip\Lang\hi.txt

C:\Program Files\7-Zip\Lang\hr.txt

C:\Program Files\7-Zip\Lang\hu.txt

C:\Program Files\7-Zip\Lang\hy.txt

C:\Program Files\7-Zip\Lang\id.txt

C:\Program Files\7-Zip\Lang\io.txt

C:\Program Files\7-Zip\Lang\is.txt

C:\Program Files\7-Zip\Lang\it.txt

C:\Program Files\7-Zip\Lang\ja.txt

C:\Program Files\7-Zip\Lang\ka.txt

C:\Program Files\7-Zip\Lang\kaa.txt

C:\Program Files\7-Zip\Lang\kk.txt

C:\Program Files\7-Zip\Lang\ko.txt

C:\Program Files\7-Zip\Lang\ku-ckb.txt

C:\Program Files\7-Zip\Lang\ku.txt

C:\Program Files\7-Zip\Lang\ky.txt

C:\Program Files\7-Zip\Lang\lij.txt

C:\Program Files\7-Zip\Lang\lt.txt

C:\Program Files\7-Zip\Lang\lv.txt

C:\Program Files\7-Zip\Lang\mk.txt

C:\Program Files\7-Zip\Lang\mn.txt

C:\Program Files\7-Zip\Lang\mng.txt

C:\Program Files\7-Zip\Lang\mng2.txt

C:\Program Files\7-Zip\Lang\mr.txt

C:\Program Files\7-Zip\Lang\ms.txt

C:\Program Files\7-Zip\Lang\nb.txt

C:\Program Files\7-Zip\Lang\ne.txt

C:\Program Files\7-Zip\Lang\nl.txt

C:\Program Files\7-Zip\Lang\nn.txt

C:\Program Files\7-Zip\Lang\pa-in.txt

C:\Program Files\7-Zip\Lang\pl.txt

C:\Program Files\7-Zip\Lang\ps.txt

C:\Program Files\7-Zip\Lang\pt-br.txt

C:\Program Files\7-Zip\Lang\pt.txt

C:\Program Files\7-Zip\Lang\ro.txt

C:\Program Files\7-Zip\Lang\ru.txt

C:\Program Files\7-Zip\Lang\sa.txt

RESOLVED APIS

kernel32.dll.OpenProcess
kernel32.dll.TerminateProcess
kernel32.dll.WriteProcessMemory
kernel32.dll.VirtualAllocEx
advapi32.dll.AdjustTokenPrivileges
user32.dll.MessageBoxTimeoutW
wintrust.dll.WinVerifyTrust
kernel32.dll.CreateProcessInternalW
ws2help.dll.WahReferenceContextByHandle
ntdll.dll.KiUserExceptionDispatcher
kernel32.dll.AddAtomA
kernel32.dll.CloseHandle
kernel32.dll.CopyFileA
kernel32.dll.CreateFileA
kernel32.dll.CreateMutexA
kernel32.dll.CreateProcessA
kernel32.dll.CreateThread
kernel32.dll.DeleteFileA
kernel32.dll.FindAtomA
kernel32.dll.GetAtomNameA
kernel32.dll.GetDriveTypeA
kernel32.dll.GetLastError
kernel32.dll.GetLocalTime
kernel32.dll.GetSystemDirectoryA
kernel32.dll.GetTempFileNameA
kernel32.dll.GetTempPathA
kernel32.dll.GetTickCount
kernel32.dll.GlobalAlloc
kernel32.dll.GlobalFree
kernel32.dll.SetErrorMode
kernel32.dll.SetFileAttributesA
kernel32.dll.Sleep
kernel32.dll.WaitForSingleObject
kernel32.dll.WriteFile

kernel32.dll.lstrcatA
kernel32.dll.lstrcmpA
kernel32.dll.lstrlenA
advapi32.dll.RegCloseKey
advapi32.dll.RegCreateKeyExA
advapi32.dll.RegOpenKeyExA
advapi32.dll.RegQueryValueExA
advapi32.dll.RegSetValueExA
msvcrt.dll.__dllonexit
msvcrt.dll._errno
msvcrt.dll._iob
msvcrt.dll.abort
msvcrt.dll.fclose
msvcrt.dll.fflush
msvcrt.dll.fopen
msvcrt.dll.fprintf
msvcrt.dll.free
msvcrt.dll.malloc
msvcrt.dll.memcpy
msvcrt.dll.memset
msvcrt.dll.rand
msvcrt.dll.srand
msvcrt.dll.strcat
msvcrt.dll._itoa
user32.dll.wsprintfA
wsock32.dll.WSAStartup
wsock32.dll.accept
wsock32.dll.bind
wsock32.dll.closesocket
wsock32.dll.connect
wsock32.dll.gethostbyname
wsock32.dll.htons
wsock32.dll.listen
wsock32.dll.recv

wsock32.dll.send
wsock32.dll.shutdown
wsock32.dll.socket
kernel32.dll.ExitProcess
kernel32.dll.LoadLibraryA
kernel32.dll.SetUnhandledExceptionFilter
msvcrt.dll.__getmainargs
msvcrt.dll.__p__environ

REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Disk\Enum
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\0
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\1
HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\vulnvol32\Version
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\vulnvol32\Version
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\iduser
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\usbactiv
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\statem
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\usw
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\pafw
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\ctfmen
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\namecp
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\software\microsoft\windows nt\currentversion\windows
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs

HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name
HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\time

EXECUTED COMMANDS

ctfmen.exe
C:\Windows\system32\smnss.exe

READ FILES

C:\Windows\System32\ctfmen.exe
C:\Windows\System32\tzres.dll
C:\Program Files\Common Files\System\symsrv.dll
C:\Windows\System32\user32.dll
C:\Users\user\AppData\Local\Temp\019c6ae7809e3c860a8d93eea365de57d128b6b9.exe
C:\Windows\System32\grcopy.dll
C:\Windows\System32\shervans.dll
C:\Windows\System32\satornas.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
\Device\KsecDD
C:\Program Files\7-Zip\History.txt
C:\Program Files\7-Zip\Lang\af.txt
C:\Program Files\7-Zip\Lang\an.txt
C:\Program Files\7-Zip\Lang\ar.txt
C:\Program Files\7-Zip\Lang\ast.txt
C:\Program Files\7-Zip\Lang\az.txt
C:\Program Files\7-Zip\Lang\ba.txt
C:\Program Files\7-Zip\Lang\be.txt
C:\Program Files\7-Zip\Lang\bg.txt
C:\Program Files\7-Zip\Lang\bn.txt
C:\Program Files\7-Zip\Lang\br.txt
C:\Program Files\7-Zip\Lang\ca.txt
C:\Program Files\7-Zip\Lang\co.txt
C:\Program Files\7-Zip\Lang\cs.txt
C:\Program Files\7-Zip\Lang\cy.txt
C:\Program Files\7-Zip\Lang\da.txt
C:\Program Files\7-Zip\Lang\de.txt

C:\Program Files\7-Zip\Lang\el.txt
C:\Program Files\7-Zip\Lang\eo.txt
C:\Program Files\7-Zip\Lang\es.txt
C:\Program Files\7-Zip\Lang\et.txt
C:\Program Files\7-Zip\Lang\eu.txt
C:\Program Files\7-Zip\Lang\ext.txt
C:\Program Files\7-Zip\Lang\fa.txt
C:\Program Files\7-Zip\Lang\fi.txt
C:\Program Files\7-Zip\Lang\fr.txt
C:\Program Files\7-Zip\Lang\fur.txt
C:\Program Files\7-Zip\Lang\fy.txt
C:\Program Files\7-Zip\Lang\ga.txt
C:\Program Files\7-Zip\Lang\gl.txt
C:\Program Files\7-Zip\Lang\gu.txt
C:\Program Files\7-Zip\Lang\he.txt
C:\Program Files\7-Zip\Lang\hi.txt
C:\Program Files\7-Zip\Lang\hr.txt
C:\Program Files\7-Zip\Lang\hu.txt
C:\Program Files\7-Zip\Lang\hy.txt
C:\Program Files\7-Zip\Lang\id.txt
C:\Program Files\7-Zip\Lang\io.txt
C:\Program Files\7-Zip\Lang\is.txt
C:\Program Files\7-Zip\Lang\it.txt
C:\Program Files\7-Zip\Lang\ja.txt
C:\Program Files\7-Zip\Lang\ka.txt
C:\Program Files\7-Zip\Lang\kaa.txt
C:\Program Files\7-Zip\Lang\kk.txt
C:\Program Files\7-Zip\Lang\ko.txt
C:\Program Files\7-Zip\Lang\ku-ckb.txt
C:\Program Files\7-Zip\Lang\ku.txt
C:\Program Files\7-Zip\Lang\ky.txt
C:\Program Files\7-Zip\Lang\lij.txt
C:\Program Files\7-Zip\Lang\lt.txt
C:\Program Files\7-Zip\Lang\lv.txt

C:\Program Files\7-Zip\Lang\mk.txt
C:\Program Files\7-Zip\Lang\mn.txt
C:\Program Files\7-Zip\Lang\mng.txt
C:\Program Files\7-Zip\Lang\mng2.txt
C:\Program Files\7-Zip\Lang\mr.txt
C:\Program Files\7-Zip\Lang\ms.txt
C:\Program Files\7-Zip\Lang\nb.txt
C:\Program Files\7-Zip\Lang\ne.txt
C:\Program Files\7-Zip\Lang\nl.txt
C:\Program Files\7-Zip\Lang\nn.txt
C:\Program Files\7-Zip\Lang\pa-in.txt
C:\Program Files\7-Zip\Lang\pl.txt
C:\Program Files\7-Zip\Lang\ps.txt
C:\Program Files\7-Zip\Lang\pt-br.txt
C:\Program Files\7-Zip\Lang\pt.txt

MUTEXES

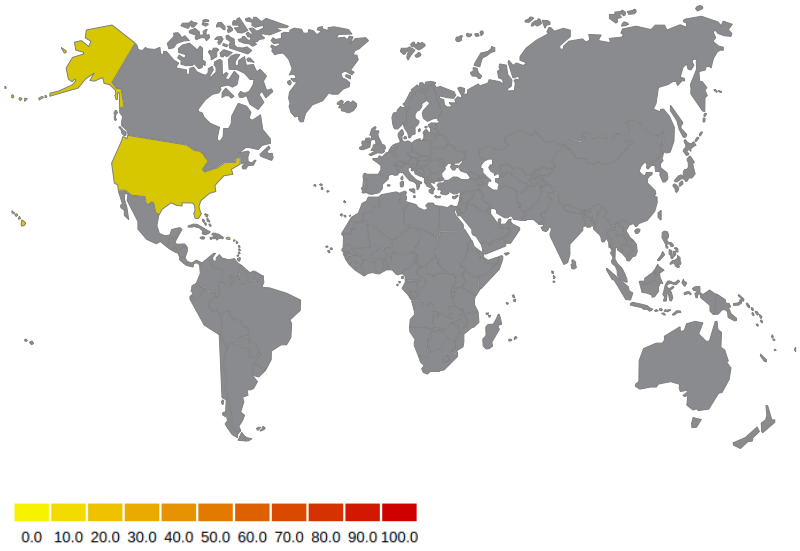
x_socks5aan
VULnaShvolna

MODIFIED REGISTRY KEYS

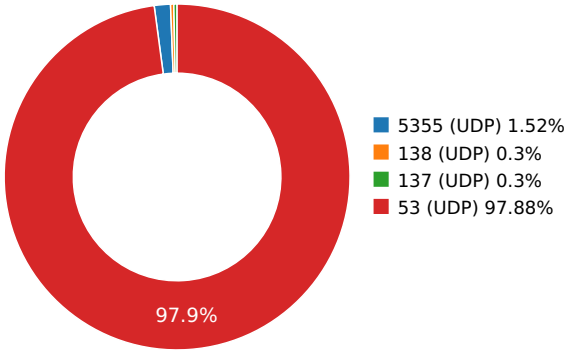
HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InprocServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InprocServer32\(Default)
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\vulnvol32\Version
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\vulnvol32\Version
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\iduser
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\usbactiv
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\statem
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\usw
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\pafw
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run\ctfmen
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\vulnvol32\Version\namecp

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
users.sourceforge.net	104.18.13.149	United States	13335	Cloudflare, Inc.	Malware Process
invincea.com	108.139.29.79	United States	16509	Amazon.com, Inc.	Malware Process
youtuber.com	104.247.82.50	Canada	206834	NEXT DIMENSION INC	Malware Process
facebook.com	157.240.245.35	United States	32934	Facebook, Inc.	Malware Process
qasqhaqwrn.info	178.162.217.107	Germany	28753	Leaseweb Deutschland Gm...	Malware Process
126.com	111.124.203.38	China	139203	CHINANET GUIZHOU PROV...	Malware Process
					Malware Process
					Malware Process
iobit.com	3.95.188.85	United States	14618	Amazon Technologies Inc.	Malware Process
gzip.org	85.187.148.2	United States	55293	Not known	Malware Process
mozilla.org	35.190.14.201	United States	15169	Google LLC	Malware Process
					Malware Process
					Malware Process
programmer.net	3.33.243.145	United States	16509	Amazon Technologies Inc.	Malware Process
unblocker.yt	199.59.243.228	United States	16509	Bodis, LLC	Malware Process
xeeR.net	64.190.63.222	United States	47846	SEDO-NET2-PI	Malware Process
megginson.com	185.199.111.153	Netherlands	54113	GitHub - 185.199.111.0/24	Malware Process
					Malware Process
gmail.com	142.251.40.101	United States	15169	Google LLC	Malware Process
www.aieov.com	96.126.123.244	United States	63949	Akamai Technologies, Inc.	Malware Process
					Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
yahoo.com	74.6.143.26	United States	26101	Oath Holdings Inc.	Malware Process
yopmail.com	87.98.250.141	United Kingdom	16276	OVH Ltd	Malware Process
mybrowserbar.com	158.85.239.244	United States	NA	SoftLayer Technologies Inc.	Malware Process
					Malware Process
					Malware Process
					Malware Process
					Malware Process
rqrawrqsqs.org	5.79.71.205	Netherlands	60781	LEASEWEB	Malware Process
esmasmqqhs.ws	64.70.19.203	United States	3561	CenturyLink Communicati...	Malware Process
rmpeaqrwwh.org	178.162.203.202	Germany	28753	Leaseweb Deutschland Gm...	Malware Process
freedownloadmanager.org	74.117.181.203	United States	40824	Webzilla Inc.	Malware Process
					Malware Process
					Malware Process
www.msftncsi.com	23.200.3.27	United States	20940	Akamai Technologies, Inc.	Malware Process
					Malware Process
courtesan.com	65.102.237.118	United States	209	CenturyLink Communicati...	Malware Process
					Malware Process
					Malware Process
					Malware Process
					Malware Process
					Malware Process
2youtube.com	208.91.196.152	Virgin Islands, British	40034	Confluence Networks Inc	Malware Process
					Malware Process
					Malware Process
					Malware Process
					Malware Process
alumni.caltech.edu	204.13.239.180	United States	19318	Interserver, Inc	Malware Process
adobee.com	103.224.182.246	Australia	133618	Trellian Pty. Limited 8 East...	Malware Process
iminent.com	52.45.106.116	United States	14618	Amazon Technologies Inc.	Malware Process
eanesaeana.ws	64.70.19.203	United States	3561	CenturyLink Communicati...	Malware Process
attbi.com	104.237.196.115	United States	20278	Nexeon Technologies, Inc.	Malware Process
faceobooks.ws	64.70.19.203	United States	3561	CenturyLink Communicati...	Malware Process
bigelowandholmes.com	208.91.197.27	United States	40034	Confluence Networks Inc	Malware Process
W9.net	185.107.56.205	Netherlands	43350	Serverhosting	Malware Process
					Malware Process
discoverypro.com	216.65.13.40	Canada	13768	Aptum Technologies	Malware Process
abc.com	18.164.96.16	United States	16509	Amazon Technologies Inc.	Malware Process

Name	IP	Country	ASN	ASN Name	Trigger Process Type
					Malware Process
example.com	93.184.215.14	Europe	15133	NETBLK-03-EU-93-184-212-...	Malware Process
adobe.com	23.200.0.43	United States	20940	Akamai Technologies, Inc.	Malware Process
mozilla.kewis.ch	178.17.170.10	Moldova, Republic of	43289	Trabia	Malware Process
flash.com	192.147.130.204	United States	15224	Adobe Systems Incorporat...	Malware Process
					Malware Process
					Malware Process
					Malware Process
					Malware Process
					Malware Process
					Malware Process
					Malware Process
					Malware Process
ShopperReports.com	13.248.169.48	United States	16509	Amazon Technologies Inc.	Malware Process

DNS QUERIES

Request	Type
5isohu.com	A
www.msftncsi.com	A
qasqhaqwrn.info	A
gmail.com	MX
www.aieov.com	A
users.sourceforge.net	MX
126.com	MX
yahoo.com	MX
mraqapeqsa.in	A
apemasmshh.com	A
mhhweqaama.in	A
qapmmrqrwa.info	A
invincea.com	MX
eanesaeana.ws	A
gzip.org	MX
rqrawrqsqs.org	A
alumni.caltech.edu	MX
megginson.com	MX
jk.uni-linz.ac.at	MX

Request	Type
cdata.tvnet.hu	MX
attbi.com	MX
courtesan.com	MX
bigelowandholmes.com	MX
smeawmehns.biz	A
2youtube.com	MX
mozilla.kewis.ch	MX
asqnannrwn.com	A
facebook.com	MX
iminent.com	MX
discoverypro.com	MX
example.com	MX
mozilla.org	MX
analytic-s.com	MX
linksicle.com	MX
youtuber.com	MX
grhjgewfewf.com	MX
faceobooks.ws	MX
youtuberie.com	MX
sqhnmhrann.biz	A
etech.com	MX
vpyekkifgv.org	MX
unblocker.yt	MX
VideoDownloadConverter_4z.com	MX
abc.com	MX
f1cc0a13-4df1-4d66-938f-088db8838882.com	MX
adsremoval.net	MX
adobee.com	MX
hansanddeta.com	MX
freedownloadmanager.org	MX
qsmapshhqh.info	A
firefox.mozilla.org	MX
nQm9l.org	MX
OKitSpace.es	MX
getpricepeep.com	MX
PackageTracer_69.com	MX
8706aaed9b904554b5cb7984e9.com	MX

Request	Type
esmasmqqhs.ws	A
mozilla.doslash.org	MX
iobit.com	MX
mybrowserbar.com	MX
test.org	MX
programmer.net	MX
2iABkVe.com	MX
W9.net	MX
rmpeaqrwwh.org	A
flash.com	MX
adobe.com	MX
ylgga.com	MX
xeeR.net	MX
yopmail.com	MX
hpyproductions.net	MX
ShopperReports.com	MX

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.04371500015	Sandbox	224.0.0.252	5355
7.04702496529	Sandbox	224.0.0.252	5355
7.10533595085	Sandbox	192.168.56.255	137
7.61415910721	Sandbox	224.0.0.252	5355
9.54430103302	Sandbox	224.0.0.252	5355
9.60939502716	Sandbox	224.0.0.252	5355
10.20038414	Sandbox	8.8.4.4	53
11.1984479427	Sandbox	8.8.8.8	53
12.105479002	Sandbox	8.8.4.4	53
13.1049389839	Sandbox	8.8.8.8	53
13.1051330566	Sandbox	192.168.56.255	138
16.3715069294	Sandbox	8.8.4.4	53
17.3704500198	Sandbox	8.8.8.8	53
18.1551971436	Sandbox	8.8.4.4	53
18.2005069256	Sandbox	8.8.4.4	53
19.152107954	Sandbox	8.8.8.8	53
19.2008509636	Sandbox	8.8.8.8	53
24.6678681374	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
25.6673150063	Sandbox	8.8.4.4	53
26.5117270947	Sandbox	8.8.8.8	53
26.5119640827	Sandbox	8.8.8.8	53
27.5111000538	Sandbox	8.8.4.4	53
27.5111169815	Sandbox	8.8.4.4	53
29.2230269909	Sandbox	8.8.8.8	53
30.2147819996	Sandbox	8.8.4.4	53
31.0431280136	Sandbox	8.8.8.8	53
31.1171331406	Sandbox	8.8.8.8	53
31.4019191265	Sandbox	8.8.8.8	53
31.6129860878	Sandbox	8.8.8.8	53
31.6770670414	Sandbox	8.8.8.8	53
32.0425429344	Sandbox	8.8.4.4	53
32.1048810482	Sandbox	8.8.4.4	53
32.4017879963	Sandbox	8.8.4.4	53
32.6050300598	Sandbox	8.8.4.4	53
32.6673870087	Sandbox	8.8.4.4	53
35.7399549484	Sandbox	8.8.8.8	53
35.8056111336	Sandbox	8.8.8.8	53
35.8711531162	Sandbox	8.8.8.8	53
35.935240984	Sandbox	8.8.8.8	53
36.7302250862	Sandbox	8.8.4.4	53
36.7925710678	Sandbox	8.8.4.4	53
36.8710279465	Sandbox	8.8.4.4	53
36.9337229729	Sandbox	8.8.4.4	53
39.0776021481	Sandbox	8.8.8.8	53
40.050796032	Sandbox	8.8.8.8	53
40.074201107	Sandbox	8.8.4.4	53
40.1493880749	Sandbox	8.8.8.8	53
40.1993341446	Sandbox	8.8.8.8	53
40.2394089699	Sandbox	8.8.8.8	53
41.0429229736	Sandbox	8.8.4.4	53
41.1362099648	Sandbox	8.8.4.4	53
41.1985781193	Sandbox	8.8.4.4	53
41.2301790714	Sandbox	8.8.4.4	53
43.4652330875	Sandbox	8.8.8.8	53
44.3514039516	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
44.451898098	Sandbox	8.8.8.8	53
44.4642591476	Sandbox	8.8.4.4	53
44.5505590439	Sandbox	8.8.8.8	53
44.647315979	Sandbox	8.8.8.8	53
45.3390219212	Sandbox	8.8.4.4	53
45.4485139847	Sandbox	8.8.4.4	53
45.5423791409	Sandbox	8.8.4.4	53
45.6362071037	Sandbox	8.8.4.4	53
48.794934988	Sandbox	8.8.8.8	53
48.7951619625	Sandbox	8.8.8.8	53
48.8338160515	Sandbox	8.8.8.8	53
48.9332270622	Sandbox	8.8.8.8	53
49.7929940224	Sandbox	8.8.4.4	53
49.7930071354	Sandbox	8.8.4.4	53
49.8238809109	Sandbox	8.8.4.4	53
49.9334659576	Sandbox	8.8.4.4	53
53.0470781326	Sandbox	8.8.8.8	53
53.0604820251	Sandbox	8.8.8.8	53
53.1271090508	Sandbox	8.8.8.8	53
53.1790721416	Sandbox	8.8.8.8	53
53.7266540527	Sandbox	8.8.8.8	53
54.0429971218	Sandbox	8.8.4.4	53
54.0580971241	Sandbox	8.8.4.4	53
54.1206150055	Sandbox	8.8.4.4	53
54.1671459675	Sandbox	8.8.4.4	53
54.7145040035	Sandbox	8.8.4.4	53
57.243694067	Sandbox	8.8.8.8	53
57.3497450352	Sandbox	8.8.8.8	53
57.3923721313	Sandbox	8.8.8.8	53
57.4791510105	Sandbox	8.8.8.8	53
57.7316961288	Sandbox	8.8.8.8	53
58.2296359539	Sandbox	8.8.4.4	53
58.3391270638	Sandbox	8.8.4.4	53
58.3862080574	Sandbox	8.8.4.4	53
58.4642920494	Sandbox	8.8.4.4	53
58.7303829193	Sandbox	8.8.4.4	53
61.6881139278	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
61.7145769596	Sandbox	8.8.8.8	53
61.8685491085	Sandbox	8.8.8.8	53
61.8776080608	Sandbox	8.8.8.8	53
62.6833329201	Sandbox	8.8.4.4	53
62.7147750854	Sandbox	8.8.4.4	53
62.8547821045	Sandbox	8.8.4.4	53
62.8704109192	Sandbox	8.8.4.4	53
66.0275359154	Sandbox	8.8.8.8	53
66.1530020237	Sandbox	8.8.8.8	53
66.1912090778	Sandbox	8.8.8.8	53
66.3082940578	Sandbox	8.8.8.8	53
67.026638031	Sandbox	8.8.4.4	53
67.1522190571	Sandbox	8.8.4.4	53
67.182954073	Sandbox	8.8.4.4	53
67.3078420162	Sandbox	8.8.4.4	53
68.1253299713	Sandbox	8.8.8.8	53
69.1204900742	Sandbox	8.8.4.4	53
70.4503390789	Sandbox	8.8.8.8	53
70.6482291222	Sandbox	8.8.8.8	53
70.8191549778	Sandbox	8.8.8.8	53
70.8251140118	Sandbox	8.8.8.8	53
71.4487500191	Sandbox	8.8.4.4	53
71.6365530491	Sandbox	8.8.4.4	53
71.8091831207	Sandbox	8.8.4.4	53
71.8233239651	Sandbox	8.8.4.4	53
71.9922139645	Sandbox	8.8.8.8	53
72.9801220894	Sandbox	8.8.4.4	53
75.1067011356	Sandbox	8.8.8.8	53
75.2283000946	Sandbox	8.8.8.8	53
75.228438139	Sandbox	8.8.8.8	53
75.3087060452	Sandbox	8.8.8.8	53
76.1414301395	Sandbox	8.8.4.4	53
76.5686900616	Sandbox	8.8.4.4	53
76.5687069893	Sandbox	8.8.4.4	53
76.5687191486	Sandbox	8.8.4.4	53
79.7005560398	Sandbox	8.8.8.8	53
79.7019720078	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
79.9335269928	Sandbox	8.8.8.8	53
79.9336180687	Sandbox	8.8.8.8	53
80.6990399361	Sandbox	8.8.4.4	53
80.6990561485	Sandbox	8.8.4.4	53
80.9328739643	Sandbox	8.8.4.4	53
80.9328889847	Sandbox	8.8.4.4	53
82.5210790634	Sandbox	8.8.8.8	53
83.5117931366	Sandbox	8.8.4.4	53
84.3219261169	Sandbox	8.8.8.8	53
84.7232310772	Sandbox	8.8.8.8	53
84.9467420578	Sandbox	8.8.8.8	53
84.9468369484	Sandbox	8.8.8.8	53
85.3082671165	Sandbox	8.8.4.4	53
85.7149441242	Sandbox	8.8.4.4	53
85.9332890511	Sandbox	8.8.4.4	53
85.9333050251	Sandbox	8.8.4.4	53
86.3367769718	Sandbox	8.8.8.8	53
87.3240871429	Sandbox	8.8.4.4	53
88.9411969185	Sandbox	8.8.8.8	53
89.0916321278	Sandbox	8.8.8.8	53
89.0916919708	Sandbox	8.8.8.8	53
89.3293349743	Sandbox	8.8.8.8	53
89.9331820011	Sandbox	8.8.4.4	53
90.0894651413	Sandbox	8.8.4.4	53
90.0894761086	Sandbox	8.8.4.4	53
90.3241169453	Sandbox	8.8.4.4	53
93.5516331196	Sandbox	8.8.8.8	53
93.6318259239	Sandbox	8.8.8.8	53
93.6320319176	Sandbox	8.8.8.8	53
94.5420839787	Sandbox	8.8.4.4	53
94.620609045	Sandbox	8.8.4.4	53
94.6206231117	Sandbox	8.8.4.4	53
100.708065987	Sandbox	8.8.8.8	53
100.794455051	Sandbox	8.8.8.8	53
101.698591948	Sandbox	8.8.4.4	53
101.792390108	Sandbox	8.8.4.4	53
112.079138994	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
113.073629141	Sandbox	8.8.4.4	53
115.167377949	Sandbox	8.8.8.8	53
115.179075003	Sandbox	8.8.8.8	53
116.151698112	Sandbox	8.8.4.4	53
116.167201996	Sandbox	8.8.4.4	53
116.84325695	Sandbox	8.8.8.8	53
116.866498947	Sandbox	8.8.8.8	53
116.871608019	Sandbox	8.8.8.8	53
117.215963125	Sandbox	8.8.8.8	53
117.839106083	Sandbox	8.8.4.4	53
117.854768038	Sandbox	8.8.4.4	53
117.870487928	Sandbox	8.8.4.4	53
118.214824915	Sandbox	8.8.4.4	53
121.492428064	Sandbox	8.8.8.8	53
121.958975077	Sandbox	8.8.8.8	53
122.066293955	Sandbox	8.8.8.8	53
122.066460133	Sandbox	8.8.8.8	53
122.49395895	Sandbox	8.8.4.4	53
122.94857502	Sandbox	8.8.4.4	53
123.058557987	Sandbox	8.8.4.4	53
123.058581114	Sandbox	8.8.4.4	53
126.310429096	Sandbox	8.8.8.8	53
126.497530937	Sandbox	8.8.8.8	53
127.308099985	Sandbox	8.8.4.4	53
127.506808043	Sandbox	8.8.4.4	53
129.402626038	Sandbox	8.8.8.8	53
129.746396065	Sandbox	8.8.8.8	53
130.401865959	Sandbox	8.8.4.4	53
130.745795012	Sandbox	8.8.4.4	53
141.997791052	Sandbox	8.8.8.8	53
141.998436928	Sandbox	8.8.8.8	53
142.995827913	Sandbox	8.8.4.4	53
142.995849133	Sandbox	8.8.4.4	53
143.672992945	Sandbox	8.8.8.8	53
144.668116093	Sandbox	8.8.4.4	53
146.640840054	Sandbox	8.8.8.8	53
147.026670933	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
147.044323921	Sandbox	8.8.8.8	53
147.044485092	Sandbox	8.8.8.8	53
147.636039972	Sandbox	8.8.4.4	53
148.011744976	Sandbox	8.8.4.4	53
148.042509079	Sandbox	8.8.4.4	53
148.042529106	Sandbox	8.8.4.4	53
148.300243139	Sandbox	8.8.8.8	53
149.292213917	Sandbox	8.8.4.4	53
151.23389101	Sandbox	8.8.8.8	53
151.620592117	Sandbox	8.8.8.8	53
151.644319057	Sandbox	8.8.8.8	53
151.654518127	Sandbox	8.8.8.8	53
152.230474949	Sandbox	8.8.4.4	53
152.620589972	Sandbox	8.8.4.4	53
152.636380911	Sandbox	8.8.4.4	53
152.652153015	Sandbox	8.8.4.4	53
155.872756004	Sandbox	8.8.8.8	53
156.352301121	Sandbox	8.8.8.8	53
156.357701063	Sandbox	8.8.8.8	53
156.372595072	Sandbox	8.8.8.8	53
156.871021986	Sandbox	8.8.4.4	53
157.339457989	Sandbox	8.8.4.4	53
157.355123997	Sandbox	8.8.4.4	53
157.370885134	Sandbox	8.8.4.4	53
157.955428123	Sandbox	8.8.8.8	53
158.949051142	Sandbox	8.8.4.4	53
160.895272017	Sandbox	8.8.8.8	53
161.289438009	Sandbox	8.8.8.8	53
161.322339058	Sandbox	8.8.8.8	53
161.342055082	Sandbox	8.8.8.8	53
161.886408091	Sandbox	8.8.4.4	53
162.276893139	Sandbox	8.8.4.4	53
162.308507919	Sandbox	8.8.4.4	53
162.339235067	Sandbox	8.8.4.4	53
162.688524961	Sandbox	8.8.8.8	53
163.682754993	Sandbox	8.8.4.4	53
165.500361919	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
166.019942999	Sandbox	8.8.8.8	53
166.019989014	Sandbox	8.8.8.8	53
166.495553017	Sandbox	8.8.4.4	53
166.498440027	Sandbox	8.8.8.8	53
167.011266947	Sandbox	8.8.4.4	53
167.011286974	Sandbox	8.8.4.4	53
167.496253014	Sandbox	8.8.4.4	53
170.497301102	Sandbox	8.8.8.8	53
170.97390008	Sandbox	8.8.8.8	53
170.989273071	Sandbox	8.8.8.8	53
171.013845921	Sandbox	8.8.8.8	53
171.495669127	Sandbox	8.8.4.4	53
171.964447021	Sandbox	8.8.4.4	53
171.980229139	Sandbox	8.8.4.4	53
172.011780024	Sandbox	8.8.4.4	53
172.456329107	Sandbox	8.8.8.8	53
173.448841095	Sandbox	8.8.4.4	53
175.562134981	Sandbox	8.8.8.8	53
175.670113087	Sandbox	8.8.8.8	53
176.045289993	Sandbox	8.8.8.8	53
176.070166111	Sandbox	8.8.8.8	53
176.558306932	Sandbox	8.8.4.4	53
176.667537928	Sandbox	8.8.4.4	53
177.043004036	Sandbox	8.8.4.4	53
177.058229923	Sandbox	8.8.4.4	53
177.090647936	Sandbox	8.8.8.8	53
178.089893103	Sandbox	8.8.4.4	53
180.076213121	Sandbox	8.8.8.8	53
180.577500105	Sandbox	8.8.8.8	53
180.577626944	Sandbox	8.8.8.8	53
180.597971916	Sandbox	8.8.8.8	53
181.073548079	Sandbox	8.8.4.4	53
181.573969126	Sandbox	8.8.4.4	53
181.573988914	Sandbox	8.8.4.4	53
181.589718103	Sandbox	8.8.4.4	53
185.092669964	Sandbox	8.8.8.8	53
185.623325109	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
185.640603065	Sandbox	8.8.8.8	53
186.089745998	Sandbox	8.8.4.4	53
186.191231012	Sandbox	8.8.8.8	53
186.62102294	Sandbox	8.8.4.4	53
186.63600111	Sandbox	8.8.4.4	53
186.734676123	Sandbox	8.8.8.8	53
187.184916019	Sandbox	8.8.4.4	53
187.729856968	Sandbox	8.8.4.4	53
190.615104914	Sandbox	8.8.8.8	53
190.622394085	Sandbox	8.8.8.8	53
190.693220139	Sandbox	8.8.8.8	53
191.228770971	Sandbox	8.8.8.8	53
191.604809999	Sandbox	8.8.4.4	53
191.62045908	Sandbox	8.8.4.4	53
191.683413029	Sandbox	8.8.4.4	53
192.214401007	Sandbox	8.8.4.4	53
195.65375495	Sandbox	8.8.8.8	53
195.802231073	Sandbox	8.8.8.8	53
196.264984131	Sandbox	8.8.8.8	53
196.265105963	Sandbox	8.8.8.8	53
196.651922941	Sandbox	8.8.4.4	53
196.792850018	Sandbox	8.8.4.4	53
196.846521139	Sandbox	8.8.8.8	53
197.261436939	Sandbox	8.8.4.4	53
197.261449099	Sandbox	8.8.4.4	53
197.839730024	Sandbox	8.8.4.4	53
200.676234961	Sandbox	8.8.8.8	53
200.687094927	Sandbox	8.8.8.8	53
201.172519922	Sandbox	8.8.8.8	53
201.277703047	Sandbox	8.8.8.8	53
201.281387091	Sandbox	8.8.8.8	53
201.667829037	Sandbox	8.8.4.4	53
201.683320999	Sandbox	8.8.4.4	53
202.167228937	Sandbox	8.8.4.4	53
202.276988983	Sandbox	8.8.4.4	53
202.276998997	Sandbox	8.8.4.4	53
205.726535082	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
206.321761131	Sandbox	8.8.8.8	53
206.330212116	Sandbox	8.8.8.8	53
206.360440016	Sandbox	8.8.8.8	53
206.714318991	Sandbox	8.8.4.4	53
207.308068037	Sandbox	8.8.4.4	53
207.323765993	Sandbox	8.8.4.4	53
207.35461998	Sandbox	8.8.4.4	53
210.011475086	Sandbox	8.8.8.8	53
210.793322086	Sandbox	8.8.8.8	53
211.011268139	Sandbox	8.8.4.4	53
211.38993001	Sandbox	8.8.8.8	53
211.419234037	Sandbox	8.8.8.8	53
211.792246103	Sandbox	8.8.4.4	53
212.030064106	Sandbox	8.8.8.8	53
212.386546135	Sandbox	8.8.4.4	53
212.417060137	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Windows\System32\Shervans.Dll	**Type :** PE32 executable (DLL) (console) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** fe082278ea5540f99dc2730739126d24 **SHA-1 :** 3b008c0e26fa11749f3ecbba9a1e6b49e39a24f3 **SHA-256 :** 53154af58974a30b6a512c80edbd28b50e718cb **SHA-512 :** 0fad5acb3a140706d26e05472f1d7122d08f94d3 **Size :** 8.704 Kilobytes.
C:\Windows\System32\Grcopy.Dll **C:\Windows\System32\Smnss.Exe**	**Type :** PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** c4f51cd1f59a1606a14210ecaf95d628 **SHA-1 :** 02c4eab457692e38b89a72f3f6c63f39ebe5f92f **SHA-256 :** 39a6b84b8a1d2eab27823e3e93ad737281f343e **SHA-512 :** cfd4e97aefd392f0bee50bea51ebc11150c5d8b3 **Size :** 199.777 Kilobytes.
C:\Windows\System32\Zipfi.Dll	**Type :** Zip archive data, at least v1.0 to extract **MD5 :** dba91744ae86d7ad49fe56926636fd94 **SHA-1 :** 468c51e2cb5554ea533707f60419049404e22af4 **SHA-256 :** 42a703c36c511fddfa6ae09830fbae3822dac1b2 **SHA-512 :** 1b125a5a2e49373199e2b4ee7fff9a2b8c5e2fb15 **Size :** 199.895 Kilobytes.
C:\Windows\System32\Zipfiaq.Dll	**Type :** Zip archive data, at least v1.0 to extract **MD5 :** 0337b96d72be88c2762c3c8ec4988c3d **SHA-1 :** 47bacda392e7c2aa618c8dfe2a20da4a95714330 **SHA-256 :** dc53e00a2c0a18893aa44e32d029f973fc69177c3 **SHA-512 :** 19eb17661277ad7392d62817fdf61d3839f73986 **Size :** 199.891 Kilobytes.
C:\Windows\System32\Satornas.Dll	**Type :** Microsoft Windows Autorun file **MD5 :** 2a5618a6231428ca8d30b5132e08c387 **SHA-1 :** 9864545905cad98ff1e482159845d50a7f55c306 **SHA-256 :** 9fc8de98ce6a939429c95ea7ddfa2bd9afd4cdc4c **SHA-512 :** 6c5be89a5ac57139f042621eba6aee0a384ef5f31 **Size :** 0.183 Kilobytes.
C:\Windows\System32\Ctfmen.Exe	**Type :** PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** 8381af4dbabee7c6e1441bf71d5621f6 **SHA-1 :** 93f187b809a11d549b3dd3cbdec1385dc0698869 **SHA-256 :** ddcff3a2263193c4593c95b7955acdf81b844db3 **SHA-512 :** 8b22463da0fea1a264a064d31609303392c310a3 **Size :** 4.16 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	virussign.com_0294f103cf2a4bf978983b54ee882ee6.exe
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
SHA1:	019c6ae7809e3c860a8d93eea365de57d128b6b9
MD5:	0294f103cf2a4bf978983b54ee882ee6
First Seen Date:	2025-01-04 21:16:41.821204 (about 15 hours ago)
Number Of Clients Seen:	2
Last Analysis Date:	2025-01-04 21:16:41.821204 (about 15 hours ago)
Human Expert Analysis Date:	2025-01-05 12:09:47.395793 (22 minutes 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	14
Trid	[]
Compilation Time Stamp	0x0 [Thu Jan 1 00:00:00 1970 UTC] [SUSPICIOUS]
Entry Point	0x4012a0 (45e3fsky)
Machine Type	Intel 386 or later - 32Bit
File Size	199777
Ssdeep	
Sha256	812bdf773194fa8e24833e37e3b82551217dc78b8ad82da3f0bb9140af4a5ace
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
45e3fsky	0x1000	0x13000	0x12600	6.55135485658	c2fae80e933ac914ad3fe864de788c40
475cokak	0x14000	0xa000	0x9c00	2.11910609727	cacd7b4fbb47f8496127ff00e5f9a37c
48f1pfcg	0x1e000	0x1000	0xa00	3.20058942264	0d8e7a6d2d4cc43befe05f8496d6761a
	0x1f000	0x1000	0xc00	5.25278825498	7b7aa1accf9d6eb83487f33fd6f402be
dMrQUrpm	0x20000	0x47c	0x600	0.763890224148	428da4f6efd2ff37eaddaed1b12452a1
wTdzgxdL	0x21000	0x4533	0x4600	5.51376677406	23e1f42df7ce9d2729e90672eb544637
EBcQahwr	0x26000	0x37	0x200	0.179432541656	7d6b92079386875cf1bfa94196ab3519
FQXfMeYO	0x27000	0xe84	0x1000	4.52363169147	a318aa7719b6cd568ca0a1e66d8297e1
hKmyjwiO	0x28000	0x11b	0x200	1.66827897619	05b2efd7846e4ba33da9846f8a833f51
PXGYXprF	0x29000	0x34b	0x400	3.74602564844	1eabda6dfce2b76cda0e1d3861dc06fb
hNfGxQeL	0x2a000	0xb9b8	0xba00	6.01031132381	4a8742251e4c3080f8d4a1a3897424bc
nSMexQnR	0x36000	0x3f0	0x400	1.29710313331	29fb822d2da95245075b7224aa5da5dc
VGiRpyFT	0x37000	0x900	0xa00	3.50196698966	b62320e01081de3a325edfb31670caed
HHmipRio	0x38000	0x2d2	0x400	3.10815148029	f3dffbccf192f6ea29ac32fc8d0333fa

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 123092, u'sha256': u'a13a5e33caed5161acd6443103d7b17069aeb6f9de04ff234a61e885fbc2547c', u'type': u'data', u'size': 744}

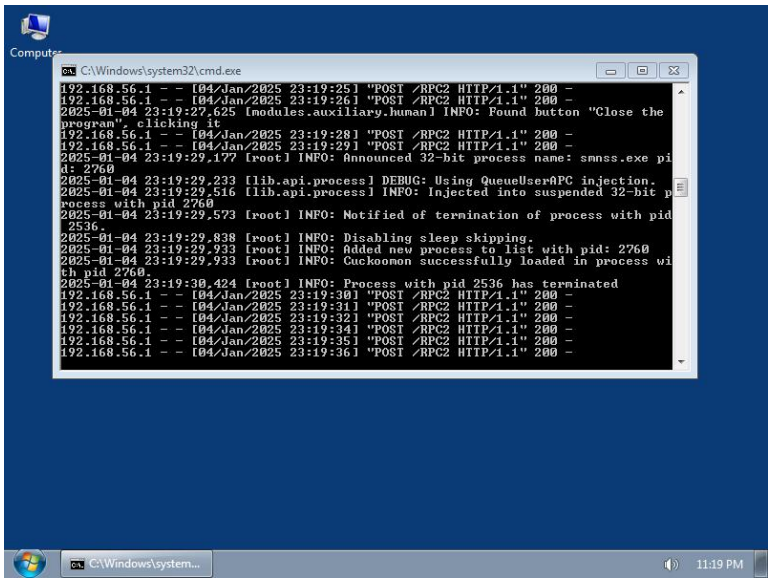
{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 123840, u'sha256': u'9325012c8f354487fbfba3d9701ae8bba76427f366ac694b7afc8e602c8ae992', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

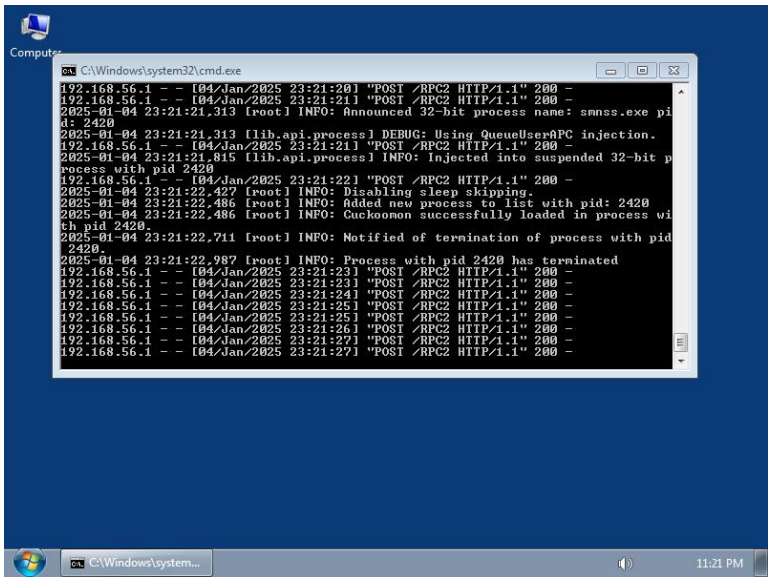
{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 124140, u'sha256': u'b10e28a32eddb2ab20a46ceae59d9c0786911eb20f0c8dd2a28421f226ea2b8b', u'type': u'MS Windows icon resource - 2 icons, 32x32, 16 colors', u'size': 34}

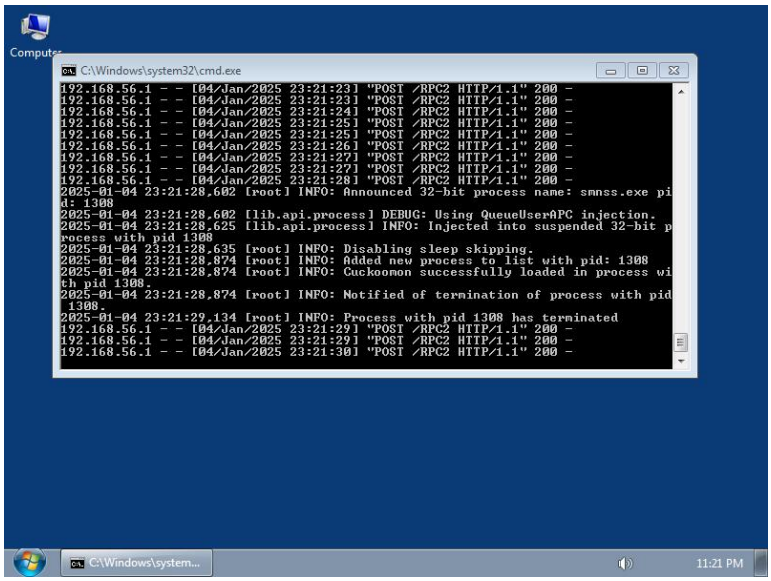
CERTIFICATE VALIDATION

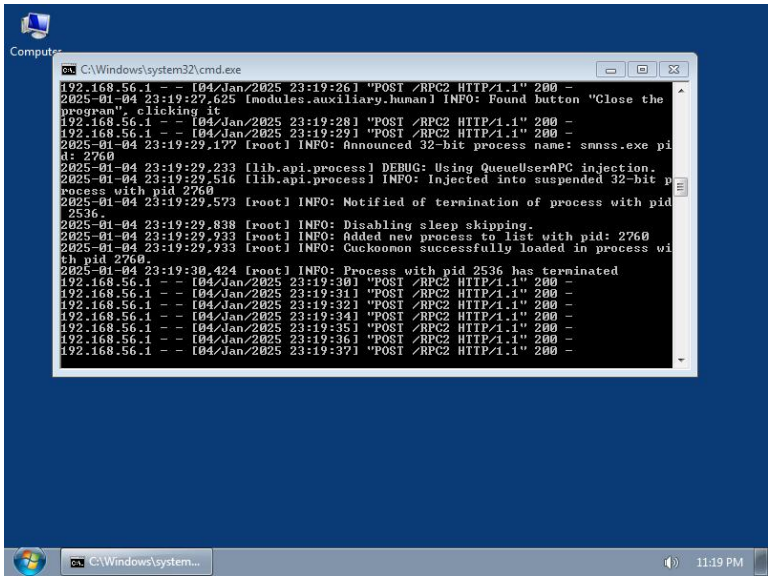
- Certificate Validation is not Applicable ?

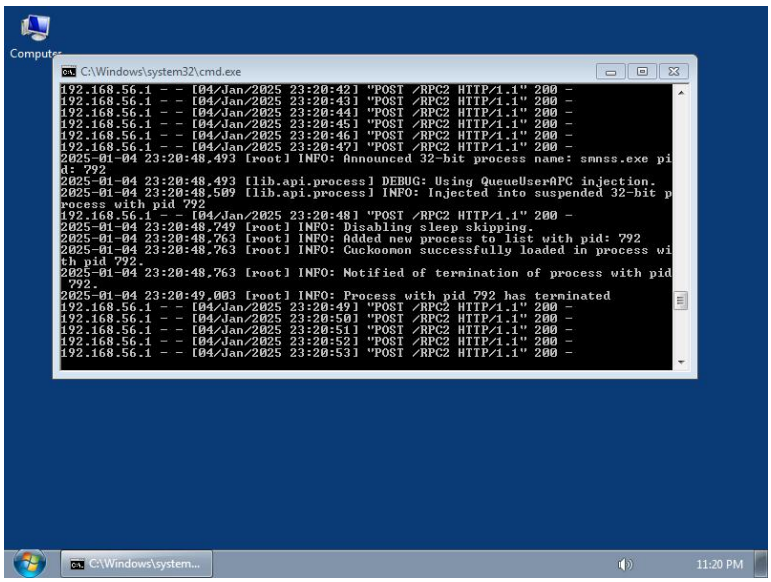
SCREENSHOTS

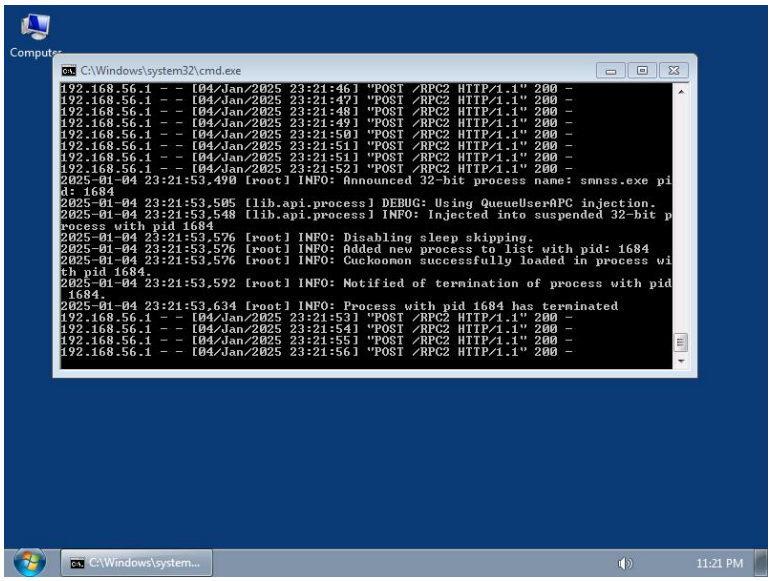


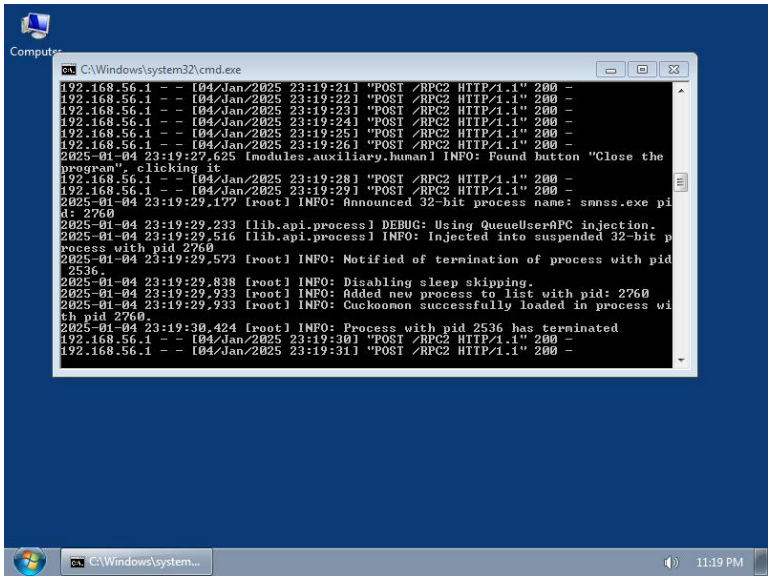


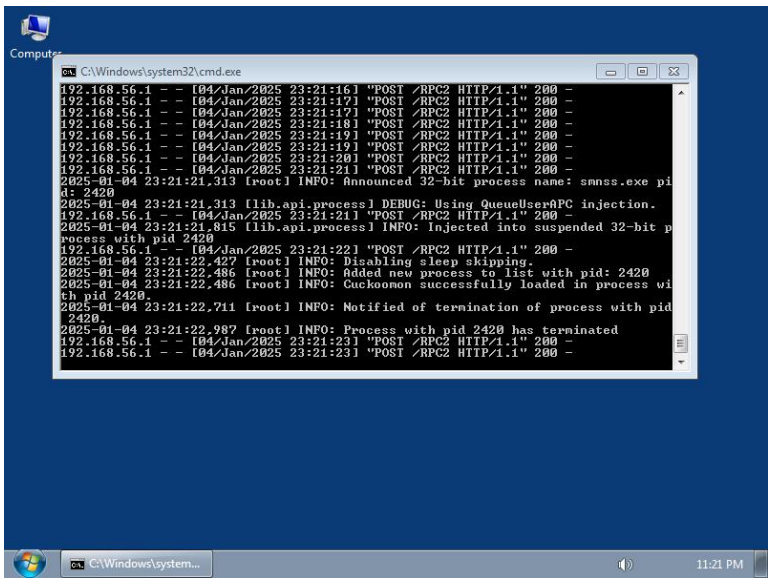

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:28] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:28,602 [root] INFO: Announced 32-bit process name: smnss.exe pid: 1308
2025-01-04 23:21:28,602 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:28,625 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 1308
2025-01-04 23:21:28,635 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:28,874 [root] INFO: Added new process to list with pid: 1308
2025-01-04 23:21:28,874 [root] INFO: Cuckoomon successfully loaded in process with pid 1308.
2025-01-04 23:21:28,874 [root] INFO: Notified of termination of process with pid 1308.
2025-01-04 23:21:29,134 [root] INFO: Process with pid 1308 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:30] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

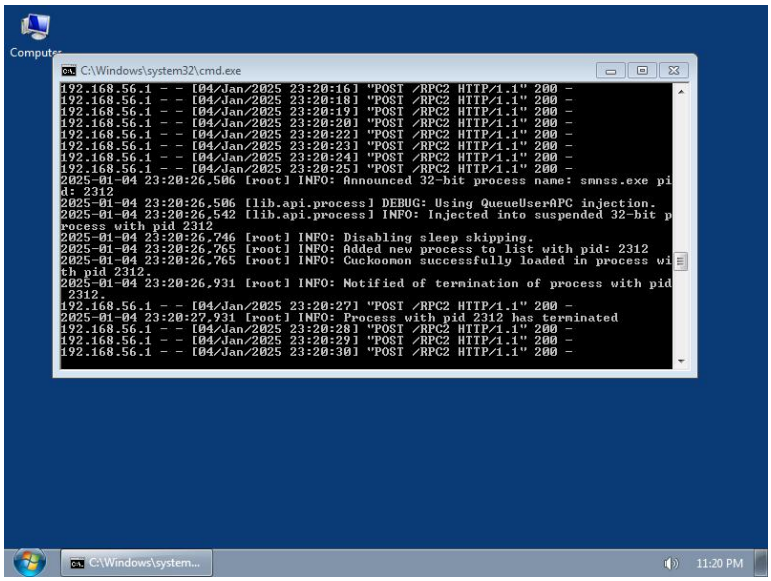

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:27,625 [modules.auxiliary.human] INFO: Found button "Close the program", clicking it
192.168.56.1 - - [04/Jan/2025 23:19:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:29] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:29,177 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2760
2025-01-04 23:19:29,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:29,516 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2760
2025-01-04 23:19:29,573 [root] INFO: Notified of termination of process with pid 2536.
2025-01-04 23:19:29,838 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:29,933 [root] INFO: Added new process to list with pid: 2760
2025-01-04 23:19:29,933 [root] INFO: Cuckoomon successfully loaded in process with pid 2760.
2025-01-04 23:19:30,424 [root] INFO: Process with pid 2536 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:37] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

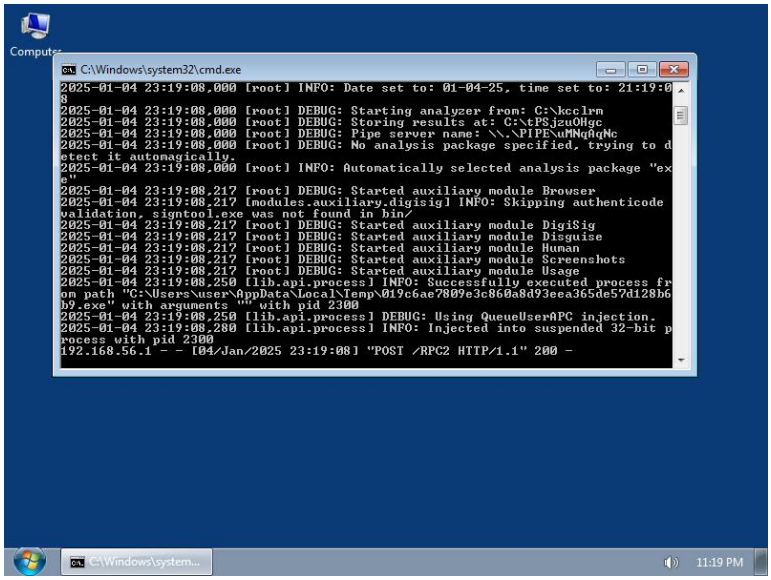

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:47] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,493 [root] INFO: Announced 32-bit process name: smnss.exe pid: 792
2025-01-04 23:20:48,493 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:48,509 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 792
192.168.56.1 - - [04/Jan/2025 23:20:48] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,749 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:48,763 [root] INFO: Added new process to list with pid: 792
2025-01-04 23:20:48,763 [root] INFO: Cuckoomon successfully loaded in process with pid 792.
2025-01-04 23:20:48,763 [root] INFO: Notified of termination of process with pid 792.
2025-01-04 23:20:49,003 [root] INFO: Process with pid 792 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:53] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

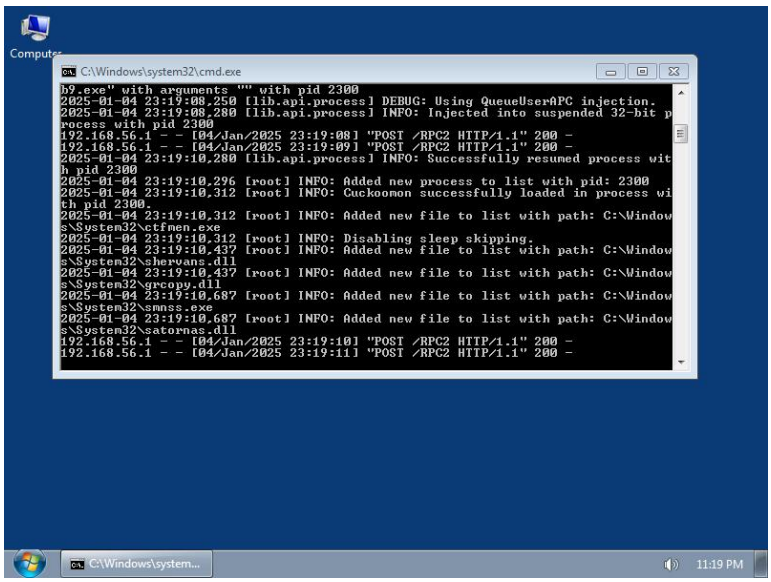

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:52] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:53,490 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1684
2025-01-04 23:21:53,505 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:53,548 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1684
2025-01-04 23:21:53,576 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:53,576 [root] INFO: Added new process to list with pid: 1684
2025-01-04 23:21:53,576 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1684.
2025-01-04 23:21:53,592 [root] INFO: Notified of termination of process with pid
 1684.
2025-01-04 23:21:53,634 [root] INFO: Process with pid 1684 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:56] "POST /RPC2 HTTP/1.1" 200 -
Computer
C:\Windows\system...
11:21 PM

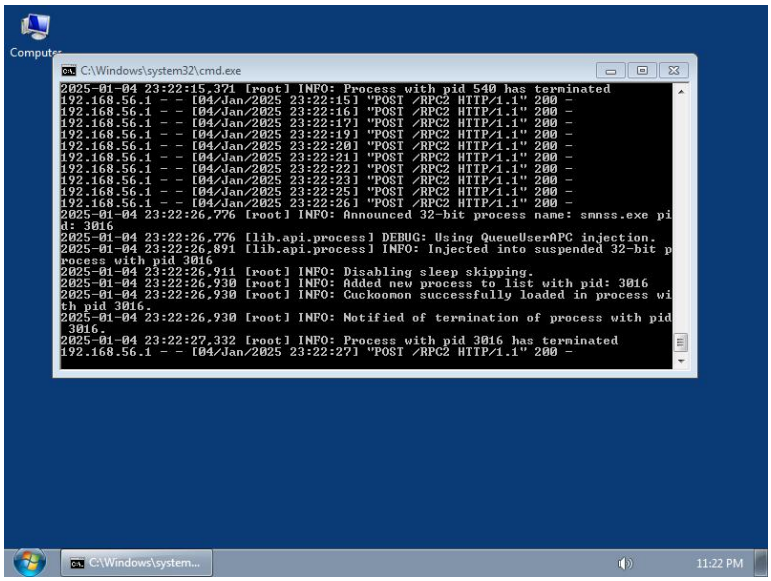

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:27,625 [modules.auxiliary.human] INFO: Found button "Close the
program", clicking it
192.168.56.1 - - [04/Jan/2025 23:19:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:29] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:29,177 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2760
2025-01-04 23:19:29,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:29,516 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2760
2025-01-04 23:19:29,573 [root] INFO: Notified of termination of process with pid
 2536.
2025-01-04 23:19:29,838 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:29,933 [root] INFO: Added new process to list with pid: 2760
2025-01-04 23:19:29,933 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2760.
2025-01-04 23:19:30,424 [root] INFO: Process with pid 2536 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:31] "POST /RPC2 HTTP/1.1" 200 -
Computer
C:\Windows\system...
11:19 PM

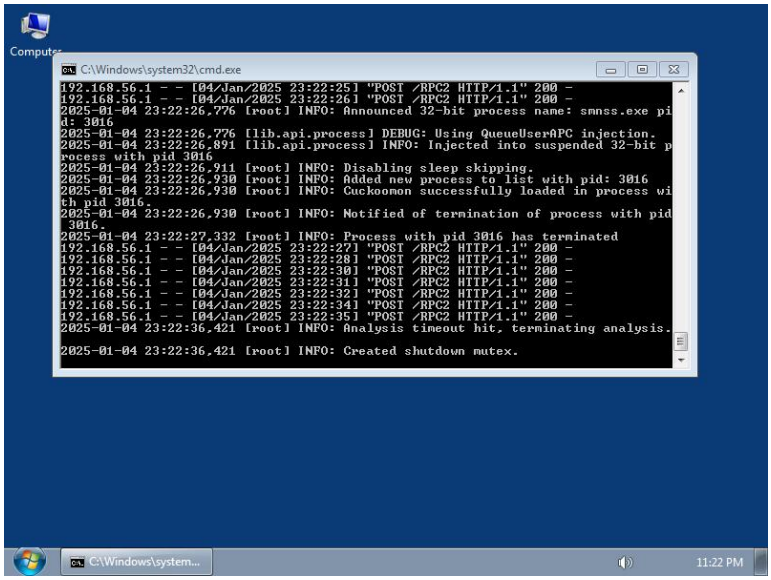

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,313 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2420
2025-01-04 23:21:21,313 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,815 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2420
192.168.56.1 - - [04/Jan/2025 23:21:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:22,427 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:22,486 [root] INFO: Added new process to list with pid: 2420
2025-01-04 23:21:22,486 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2420.
2025-01-04 23:21:22,711 [root] INFO: Notified of termination of process with pid
 2420.
2025-01-04 23:21:22,987 [root] INFO: Process with pid 2420 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
Computer
C:\Windows\system...
11:21 PM

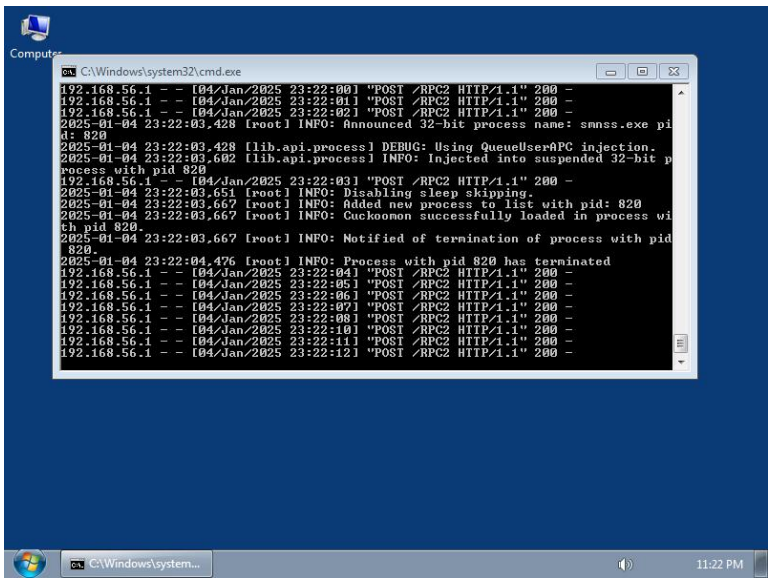

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:25] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:26,506 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2312
2025-01-04 23:20:26,506 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:26,542 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2312
2025-01-04 23:20:26,746 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:26,765 [root] INFO: Added new process to list with pid: 2312
2025-01-04 23:20:26,765 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2312.
2025-01-04 23:20:26,931 [root] INFO: Notified of termination of process with pid
 2312.
192.168.56.1 - - [04/Jan/2025 23:20:27] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:27,931 [root] INFO: Process with pid 2312 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:30] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

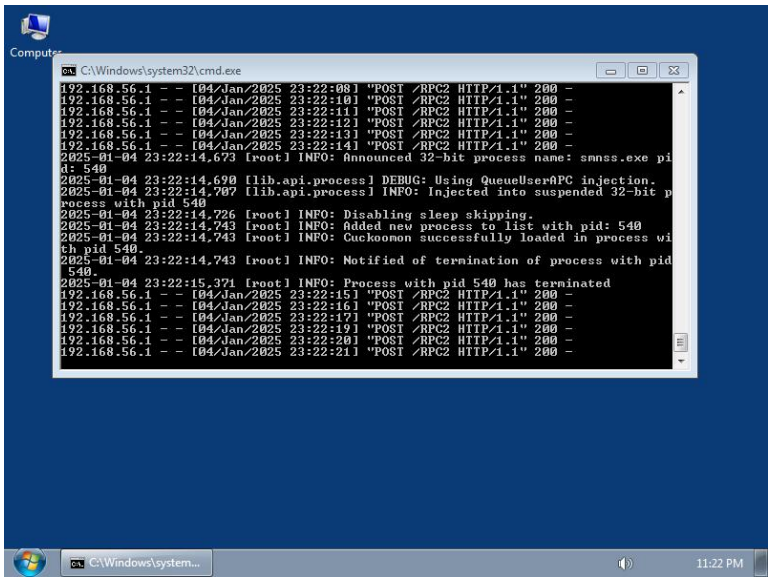

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:19:08,000 [root] INFO: Date set to: 01-04-25, time set to: 21:19:0
8
2025-01-04 23:19:08,000 [root] DEBUG: Starting analyzer from: C:\kcclrm
2025-01-04 23:19:08,000 [root] DEBUG: Storing results at: C:\tPSjzuOHgc
2025-01-04 23:19:08,000 [root] DEBUG: Pipe server name: \\.\PIPE\uMNqRqNc
2025-01-04 23:19:08,000 [root] DEBUG: No analysis package specified, trying to d
etect it automagically.
2025-01-04 23:19:08,000 [root] INFO: Automatically selected analysis package "ex
e"
2025-01-04 23:19:08,217 [root] DEBUG: Started auxiliary module Browser
2025-01-04 23:19:08,217 [modules.auxiliary.digisig] INFO: Skipping authenticode
validation, signtool.exe was not found in bin/
2025-01-04 23:19:08,217 [root] DEBUG: Started auxiliary module DigiSig
2025-01-04 23:19:08,217 [root] DEBUG: Started auxiliary module Disguise
2025-01-04 23:19:08,217 [root] DEBUG: Started auxiliary module Human
2025-01-04 23:19:08,217 [root] DEBUG: Started auxiliary module Screenshots
2025-01-04 23:19:08,217 [root] DEBUG: Started auxiliary module Usage
2025-01-04 23:19:08,250 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\019c6ae7809e3c860a8d93eea365de57d128b6
b9.exe" with arguments "" with pid 2300
2025-01-04 23:19:08,250 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:08,280 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2300
192.168.56.1 - - [04/Jan/2025 23:19:08] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

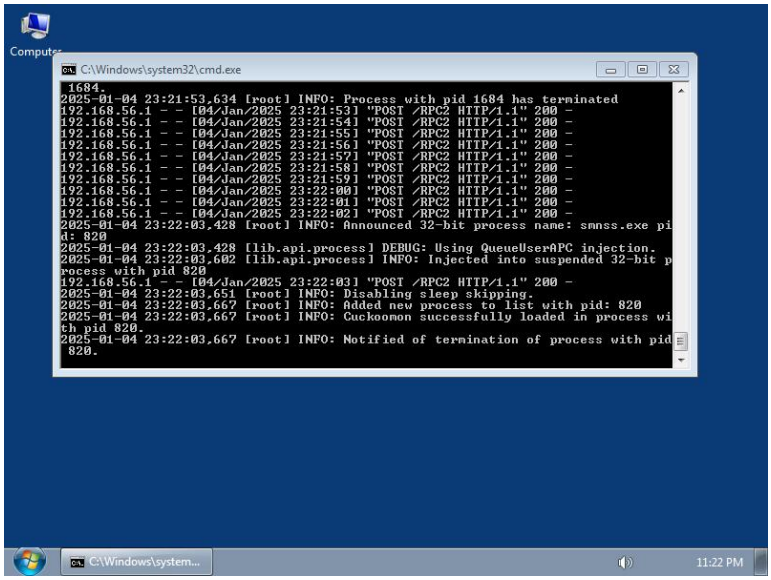

Computer
C:\Windows\system32\cmd.exe
b9.exe" with arguments "" with pid 2300
2025-01-04 23:19:08,250 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:08,280 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2300
192.168.56.1 - - [04/Jan/2025 23:19:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:09] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:10,280 [lib.api.process] INFO: Successfully resumed process wit
h pid 2300
2025-01-04 23:19:10,296 [root] INFO: Added new process to list with pid: 2300
2025-01-04 23:19:10,312 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2300.
2025-01-04 23:19:10,312 [root] INFO: Added new file to list with path: C:\Window
s\System32\ctfmen.exe
2025-01-04 23:19:10,312 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:10,437 [root] INFO: Added new file to list with path: C:\Window
s\System32\shervans.dll
2025-01-04 23:19:10,437 [root] INFO: Added new file to list with path: C:\Window
s\System32\grcopy.dll
2025-01-04 23:19:10,687 [root] INFO: Added new file to list with path: C:\Window
s\System32\smnss.exe
2025-01-04 23:19:10,687 [root] INFO: Added new file to list with path: C:\Window
s\System32\satornas.dll
192.168.56.1 - - [04/Jan/2025 23:19:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:11] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

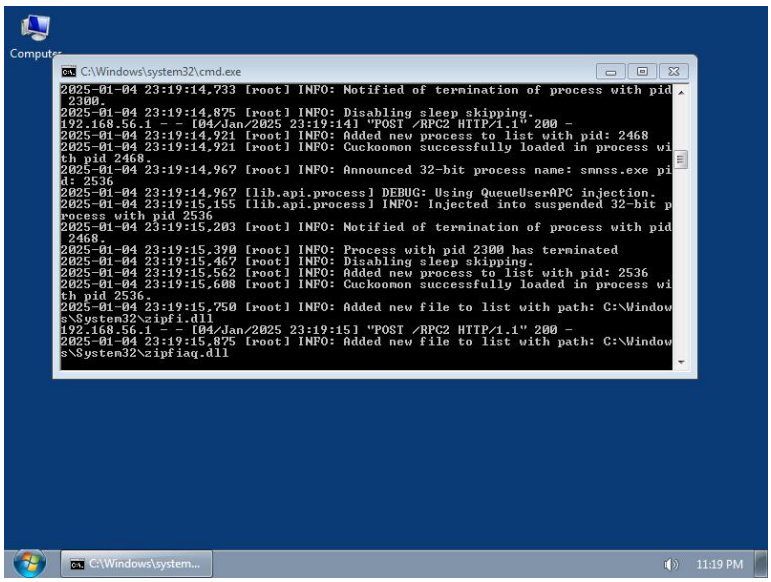

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:22:15,371 [root] INFO: Process with pid 540 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:26,776 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3016
2025-01-04 23:22:26,776 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:26,891 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3016
2025-01-04 23:22:26,911 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:26,930 [root] INFO: Added new process to list with pid: 3016
2025-01-04 23:22:26,930 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3016.
2025-01-04 23:22:26,930 [root] INFO: Notified of termination of process with pid
 3016.
2025-01-04 23:22:27,332 [root] INFO: Process with pid 3016 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:27] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

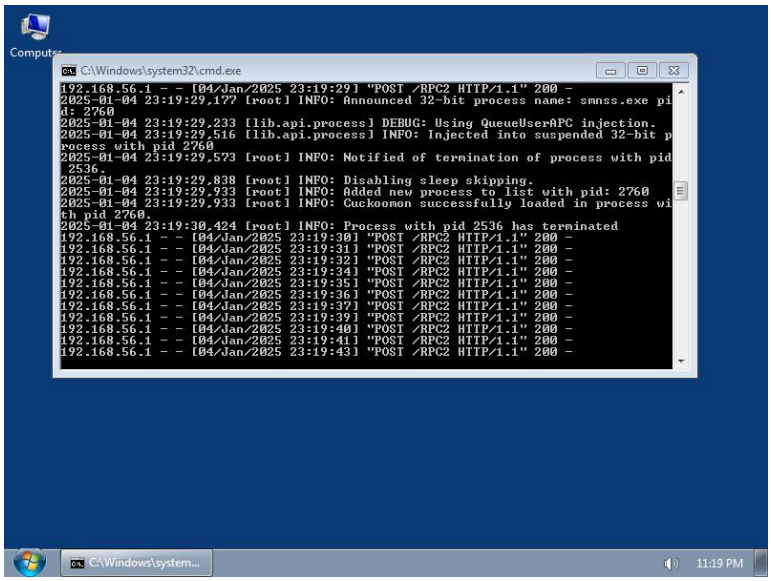

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:26,776 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3016
2025-01-04 23:22:26,776 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:26,891 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3016
2025-01-04 23:22:26,911 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:26,930 [root] INFO: Added new process to list with pid: 3016
2025-01-04 23:22:26,930 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3016.
2025-01-04 23:22:26,930 [root] INFO: Notified of termination of process with pid
 3016.
2025-01-04 23:22:27,332 [root] INFO: Process with pid 3016 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:35] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:36,421 [root] INFO: Analysis timeout hit, terminating analysis.
2025-01-04 23:22:36,421 [root] INFO: Created shutdown mutex.
C:\Windows\system...
11:22 PM

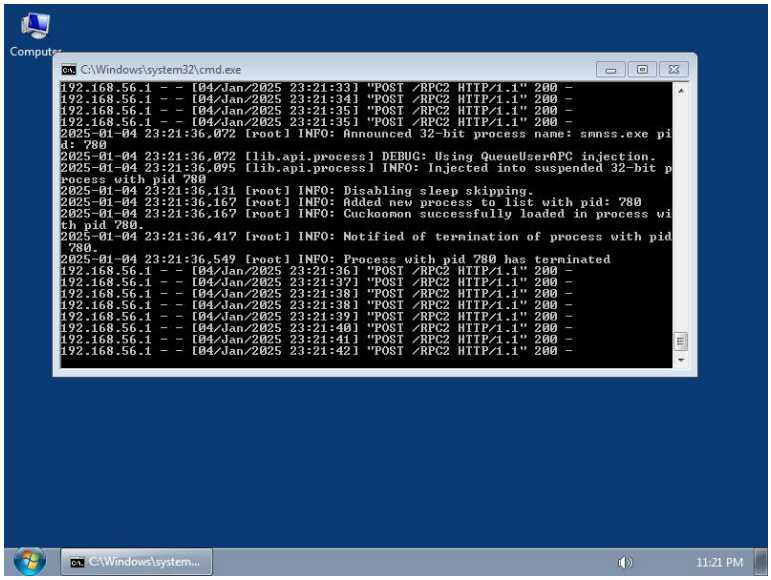

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:02] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,428 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 820
2025-01-04 23:22:03,428 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:03,602 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 820
192.168.56.1 - - [04/Jan/2025 23:22:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,651 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:03,667 [root] INFO: Added new process to list with pid: 820
2025-01-04 23:22:03,667 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 820.
2025-01-04 23:22:03,667 [root] INFO: Notified of termination of process with pid
 820.
2025-01-04 23:22:04,476 [root] INFO: Process with pid 820 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:12] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

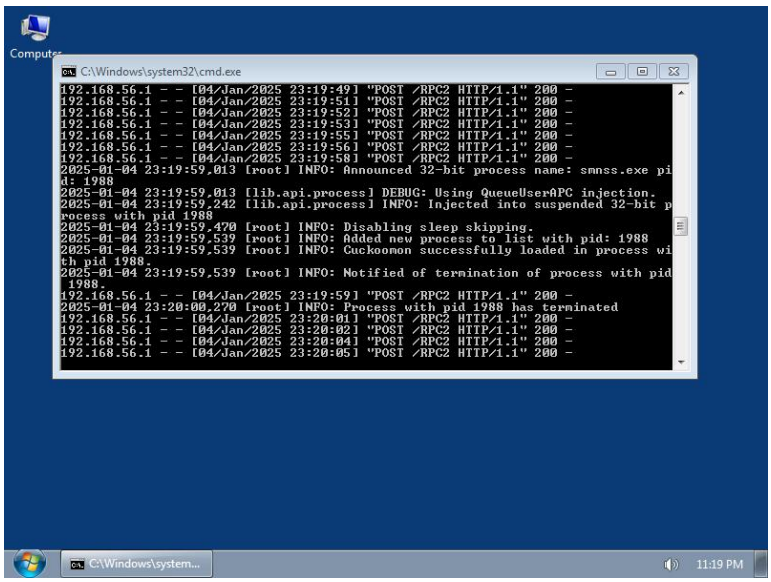

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:14,673 [root] INFO: Announced 32-bit process name: smnss.exe pid: 540
2025-01-04 23:22:14,690 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:14,707 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 540
2025-01-04 23:22:14,726 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:14,743 [root] INFO: Added new process to list with pid: 540
2025-01-04 23:22:14,743 [root] INFO: Cuckoomon successfully loaded in process with pid 540.
2025-01-04 23:22:14,743 [root] INFO: Notified of termination of process with pid 540.
2025-01-04 23:22:15,371 [root] INFO: Process with pid 540 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:21] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

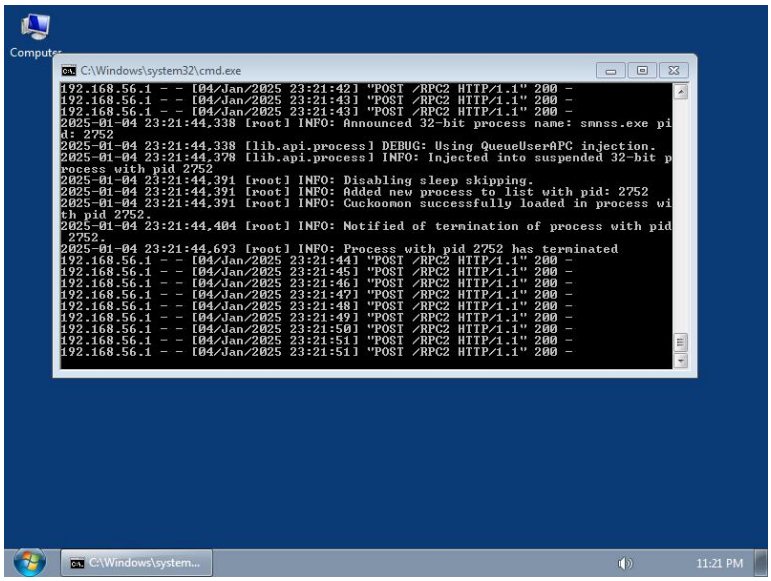

Computer
C:\Windows\system32\cmd.exe
1684.
2025-01-04 23:21:53,634 [root] INFO: Process with pid 1684 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:02] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,428 [root] INFO: Announced 32-bit process name: smnss.exe pid: 820
2025-01-04 23:22:03,428 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:03,602 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 820
192.168.56.1 - - [04/Jan/2025 23:22:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,651 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:03,667 [root] INFO: Added new process to list with pid: 820
2025-01-04 23:22:03,667 [root] INFO: Cuckoomon successfully loaded in process with pid 820.
2025-01-04 23:22:03,667 [root] INFO: Notified of termination of process with pid 820.
C:\Windows\system...
11:22 PM

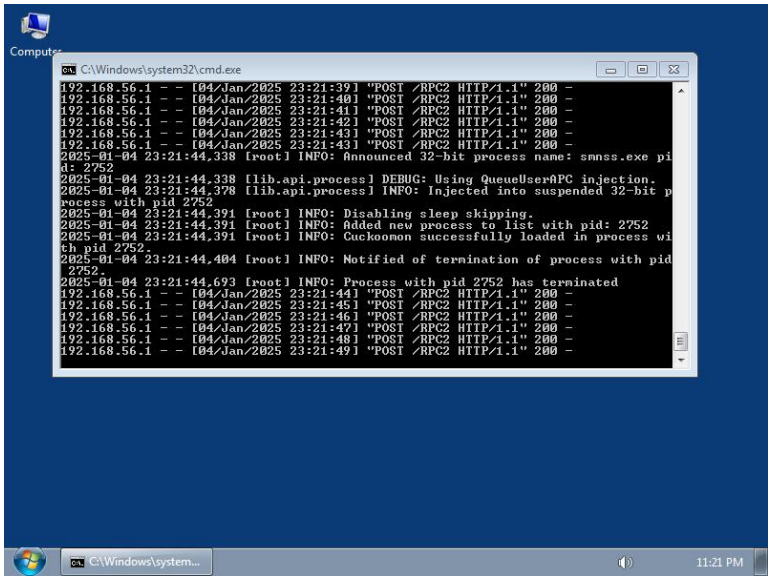

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:19:14,733 [root] INFO: Notified of termination of process with pid 2300.
2025-01-04 23:19:14,875 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [04/Jan/2025 23:19:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:14,921 [root] INFO: Added new process to list with pid: 2468
2025-01-04 23:19:14,921 [root] INFO: Cuckoomon successfully loaded in process with pid 2468.
2025-01-04 23:19:14,967 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2536
2025-01-04 23:19:14,967 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:15,155 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2536
2025-01-04 23:19:15,203 [root] INFO: Notified of termination of process with pid 2468.
2025-01-04 23:19:15,390 [root] INFO: Process with pid 2300 has terminated
2025-01-04 23:19:15,467 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:15,562 [root] INFO: Added new process to list with pid: 2536
2025-01-04 23:19:15,608 [root] INFO: Cuckoomon successfully loaded in process with pid 2536.
2025-01-04 23:19:15,750 [root] INFO: Added new file to list with path: C:\Windows\System32\zipfi.dll
192.168.56.1 - - [04/Jan/2025 23:19:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:15,875 [root] INFO: Added new file to list with path: C:\Windows\System32\zipfiaq.dll
C:\Windows\system...
11:19 PM

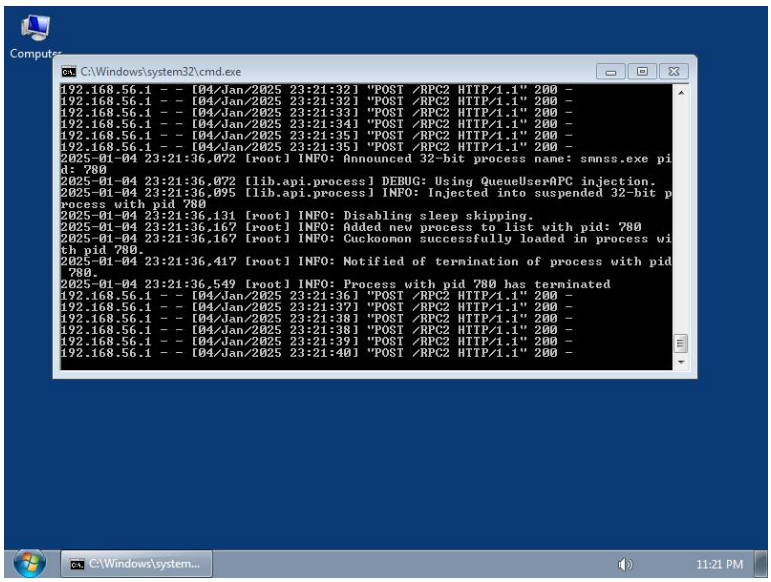

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:29] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:29,177 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2760
2025-01-04 23:19:29,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:29,516 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2760
2025-01-04 23:19:29,573 [root] INFO: Notified of termination of process with pid 2536.
2025-01-04 23:19:29,838 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:29,933 [root] INFO: Added new process to list with pid: 2760
2025-01-04 23:19:29,933 [root] INFO: Cuckoomon successfully loaded in process with pid 2760.
2025-01-04 23:19:30,424 [root] INFO: Process with pid 2536 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:43] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

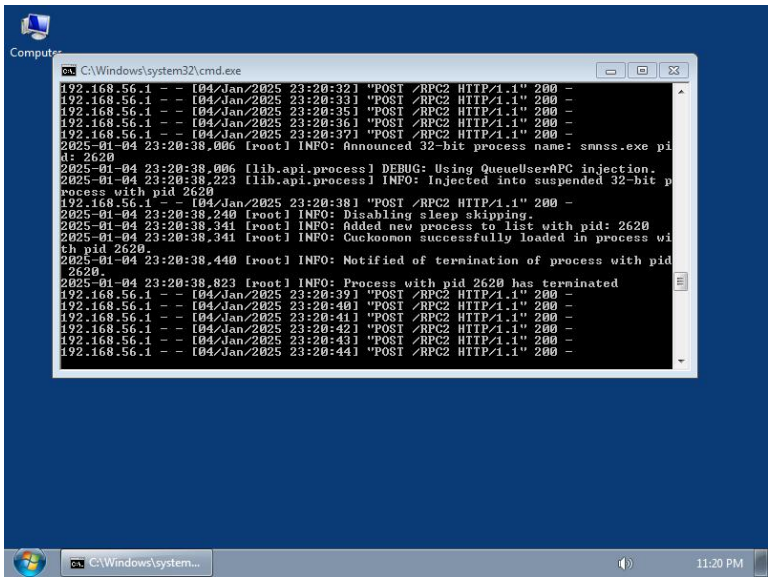

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:36,072 [root] INFO: Announced 32-bit process name: smnss.exe pid: 780
2025-01-04 23:21:36,072 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:36,095 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 780
2025-01-04 23:21:36,131 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:36,167 [root] INFO: Added new process to list with pid: 780
2025-01-04 23:21:36,167 [root] INFO: Cuckoomon successfully loaded in process with pid 780.
2025-01-04 23:21:36,417 [root] INFO: Notified of termination of process with pid 780.
2025-01-04 23:21:36,549 [root] INFO: Process with pid 780 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:42] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

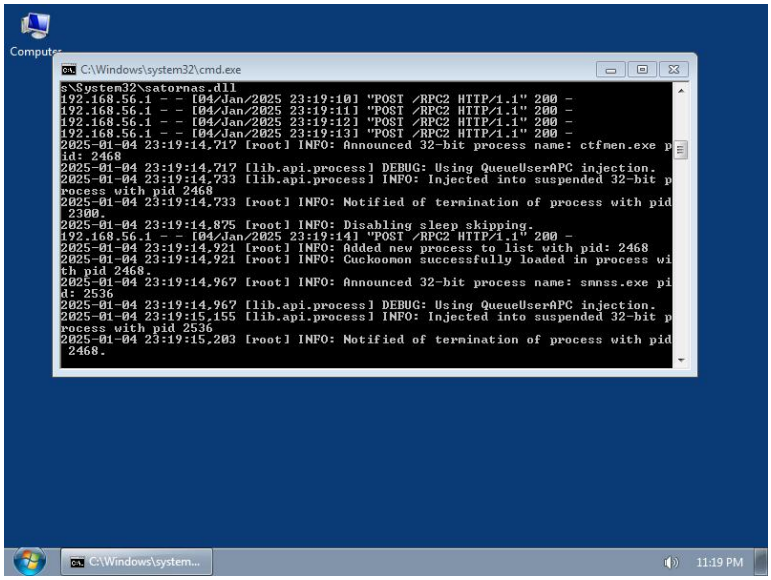

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:59,013 [root] INFO: Announced 32-bit process name: smnss.exe pid: 1988
2025-01-04 23:19:59,013 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:59,242 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 1988
2025-01-04 23:19:59,470 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:59,539 [root] INFO: Added new process to list with pid: 1988
2025-01-04 23:19:59,539 [root] INFO: Cuckoomon successfully loaded in process with pid 1988.
2025-01-04 23:19:59,539 [root] INFO: Notified of termination of process with pid 1988.
192.168.56.1 - - [04/Jan/2025 23:19:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:00,270 [root] INFO: Process with pid 1988 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:05] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

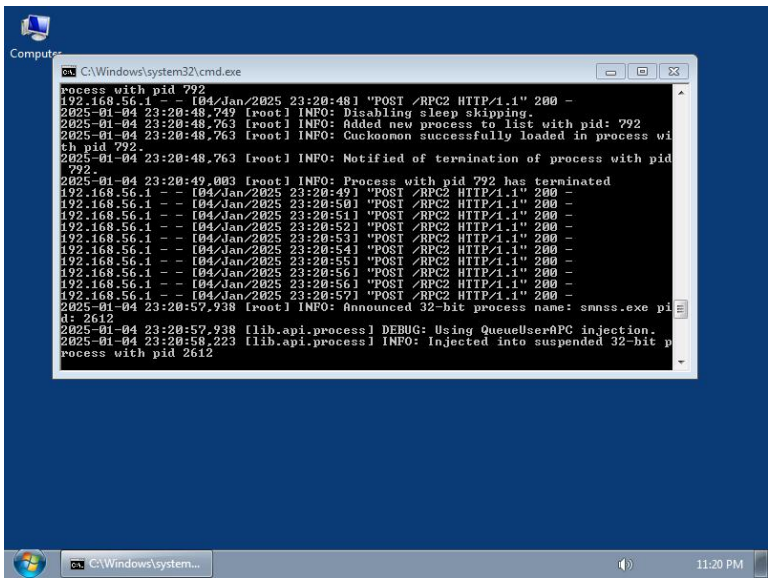

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:44,338 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2752
2025-01-04 23:21:44,338 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:44,378 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2752
2025-01-04 23:21:44,391 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:44,391 [root] INFO: Added new process to list with pid: 2752
2025-01-04 23:21:44,391 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2752.
2025-01-04 23:21:44,404 [root] INFO: Notified of termination of process with pid
 2752.
2025-01-04 23:21:44,693 [root] INFO: Process with pid 2752 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
Computer
C:\Windows\system...
11:21 PM

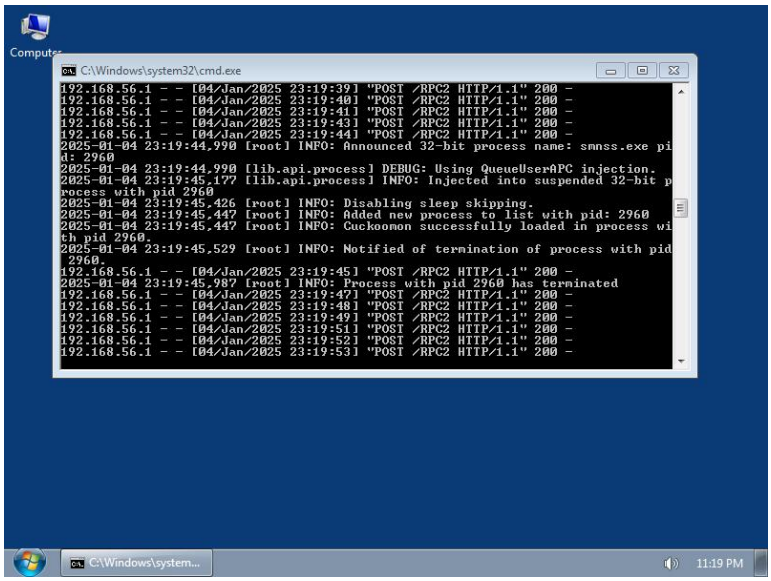

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:44,338 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2752
2025-01-04 23:21:44,338 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:44,378 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2752
2025-01-04 23:21:44,391 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:44,391 [root] INFO: Added new process to list with pid: 2752
2025-01-04 23:21:44,391 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2752.
2025-01-04 23:21:44,404 [root] INFO: Notified of termination of process with pid
 2752.
2025-01-04 23:21:44,693 [root] INFO: Process with pid 2752 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:49] "POST /RPC2 HTTP/1.1" 200 -
Computer
C:\Windows\system...
11:21 PM

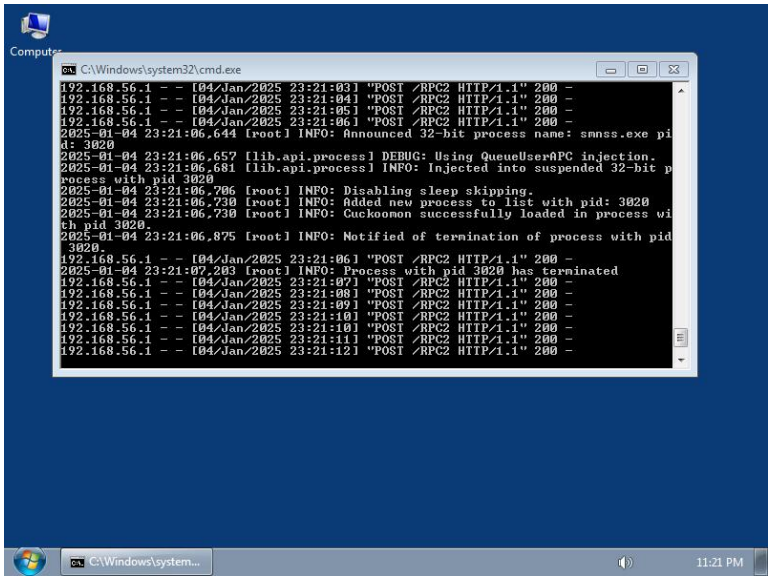

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:36,072 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 780
2025-01-04 23:21:36,072 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:36,095 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 780
2025-01-04 23:21:36,131 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:36,167 [root] INFO: Added new process to list with pid: 780
2025-01-04 23:21:36,167 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 780.
2025-01-04 23:21:36,417 [root] INFO: Notified of termination of process with pid
 780.
2025-01-04 23:21:36,549 [root] INFO: Process with pid 780 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:40] "POST /RPC2 HTTP/1.1" 200 -
Computer
C:\Windows\system...
11:21 PM

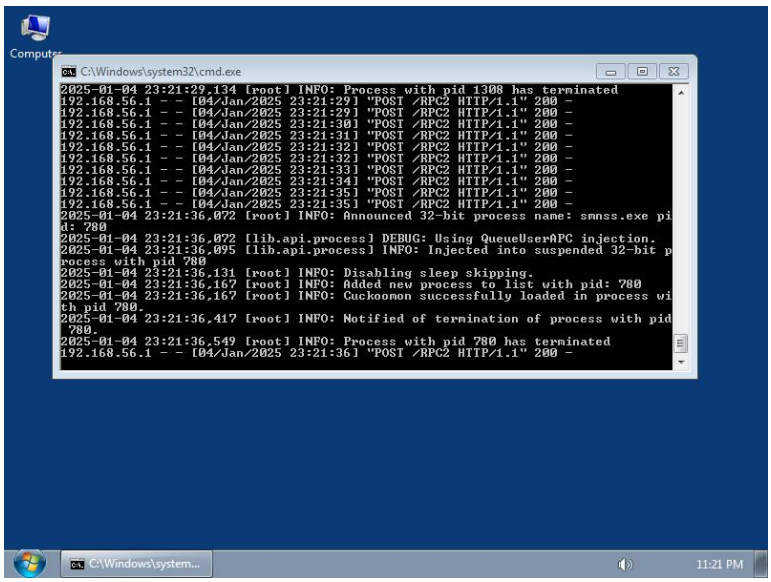

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:37] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,006 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2620
2025-01-04 23:20:38,006 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:38,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2620
192.168.56.1 - - [04/Jan/2025 23:20:38] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,240 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:38,341 [root] INFO: Added new process to list with pid: 2620
2025-01-04 23:20:38,341 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2620.
2025-01-04 23:20:38,440 [root] INFO: Notified of termination of process with pid
 2620.
2025-01-04 23:20:38,823 [root] INFO: Process with pid 2620 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:44] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

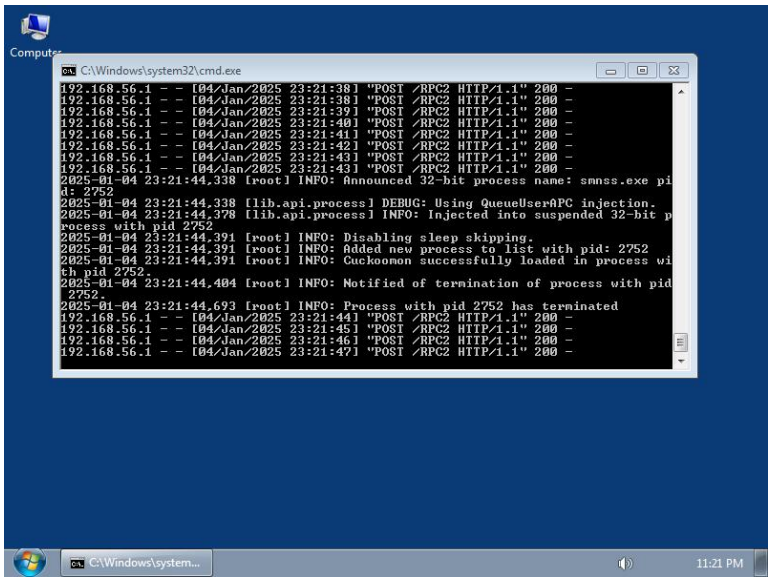

Computer
C:\Windows\system32\cmd.exe
s\System32\satornas.dll
192.168.56.1 - - [04/Jan/2025 23:19:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:13] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:14,717 [root] INFO: Announced 32-bit process name: ctfmen.exe p
id: 2468
2025-01-04 23:19:14,717 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:14,733 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2468
2025-01-04 23:19:14,733 [root] INFO: Notified of termination of process with pid
 2300.
2025-01-04 23:19:14,875 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [04/Jan/2025 23:19:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:14,921 [root] INFO: Added new process to list with pid: 2468
2025-01-04 23:19:14,921 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2468.
2025-01-04 23:19:14,967 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2536
2025-01-04 23:19:14,967 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:15,155 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2536
2025-01-04 23:19:15,203 [root] INFO: Notified of termination of process with pid
 2468.
C:\Windows\system...
11:19 PM

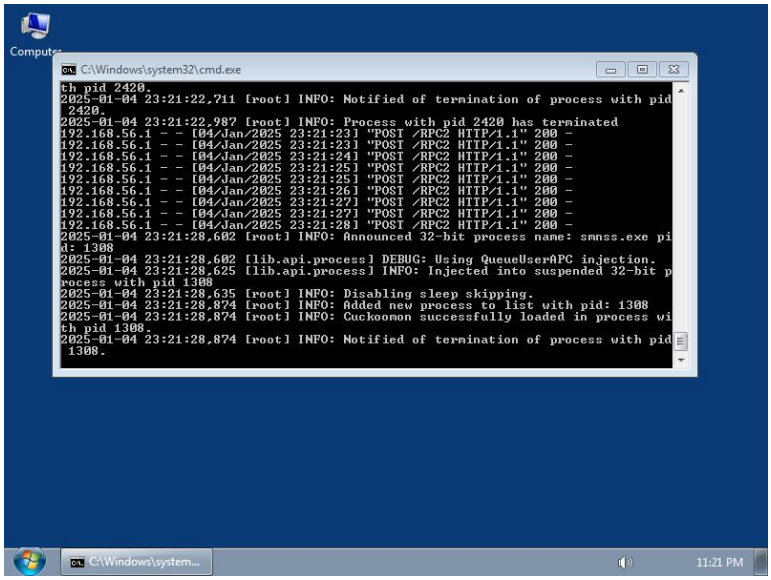

Computer
C:\Windows\system32\cmd.exe
rocess with pid 792
192.168.56.1 - - [04/Jan/2025 23:20:48] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,749 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:48,763 [root] INFO: Added new process to list with pid: 792
2025-01-04 23:20:48,763 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 792.
2025-01-04 23:20:48,763 [root] INFO: Notified of termination of process with pid
 792.
2025-01-04 23:20:49,003 [root] INFO: Process with pid 792 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:57] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:57,938 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2612
2025-01-04 23:20:57,938 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:58,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2612
C:\Windows\system...
11:20 PM

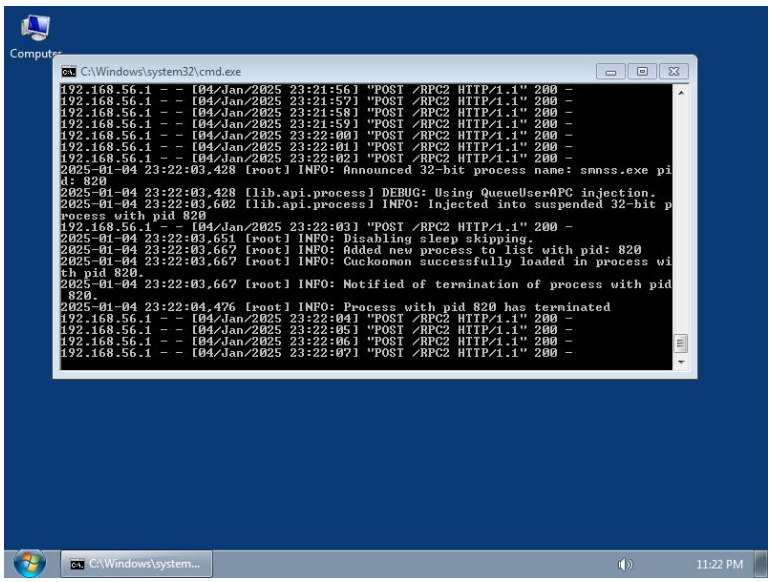

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:44] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:44,990 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2960
2025-01-04 23:19:44,990 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:45,177 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2960
2025-01-04 23:19:45,426 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:45,447 [root] INFO: Added new process to list with pid: 2960
2025-01-04 23:19:45,447 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2960.
2025-01-04 23:19:45,529 [root] INFO: Notified of termination of process with pid
 2960.
192.168.56.1 - - [04/Jan/2025 23:19:45] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:45,987 [root] INFO: Process with pid 2960 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:53] "POST /RPC2 HTTP/1.1" 200 -
Computer
C:\Windows\system...
11:19 PM

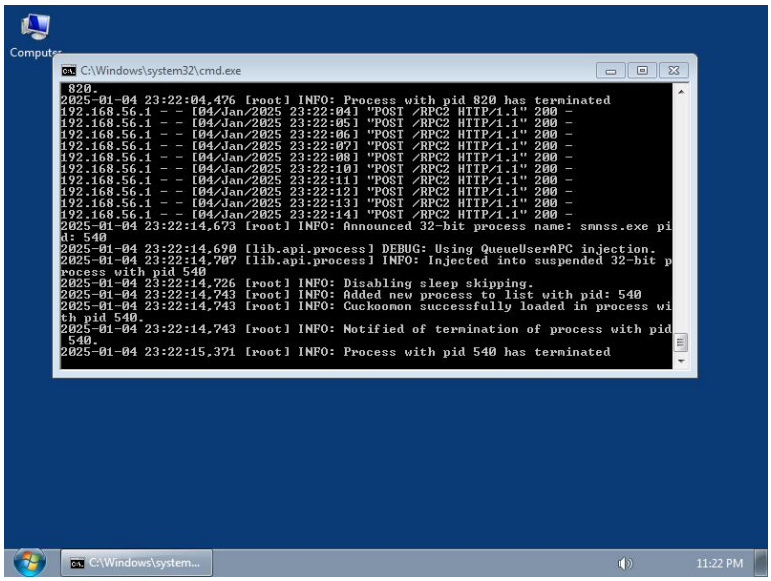

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:06,644 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3020
2025-01-04 23:21:06,657 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:06,681 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3020
2025-01-04 23:21:06,706 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:06,730 [root] INFO: Added new process to list with pid: 3020
2025-01-04 23:21:06,730 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3020.
2025-01-04 23:21:06,875 [root] INFO: Notified of termination of process with pid
 3020.
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:07,203 [root] INFO: Process with pid 3020 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
Computer
C:\Windows\system...
11:21 PM

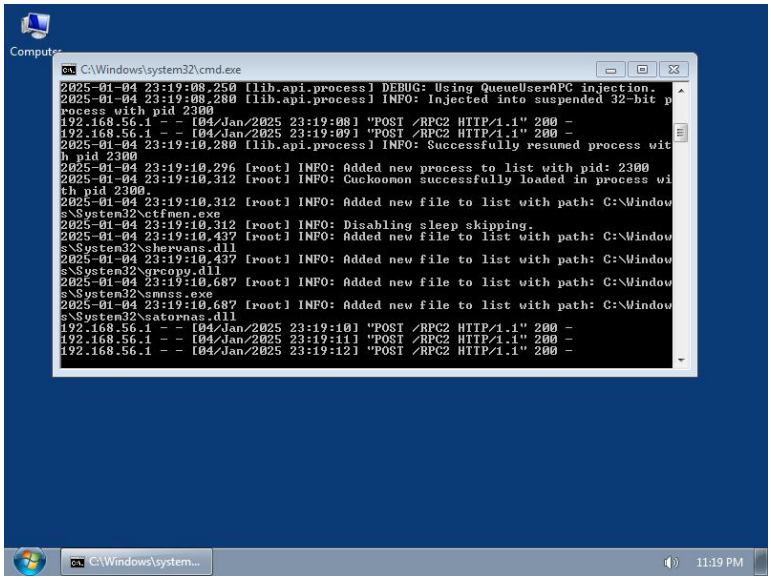

C:\Windows\system32\cmd.exe
2025-01-04 23:21:29,134 [root] INFO: Process with pid 1308 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:36,072 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 780
2025-01-04 23:21:36,072 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:36,095 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 780
2025-01-04 23:21:36,131 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:36,167 [root] INFO: Added new process to list with pid: 780
2025-01-04 23:21:36,167 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 780.
2025-01-04 23:21:36,417 [root] INFO: Notified of termination of process with pid
 780.
2025-01-04 23:21:36,549 [root] INFO: Process with pid 780 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:36] "POST /RPC2 HTTP/1.1" 200 -
Computer
C:\Windows\system...
11:21 PM

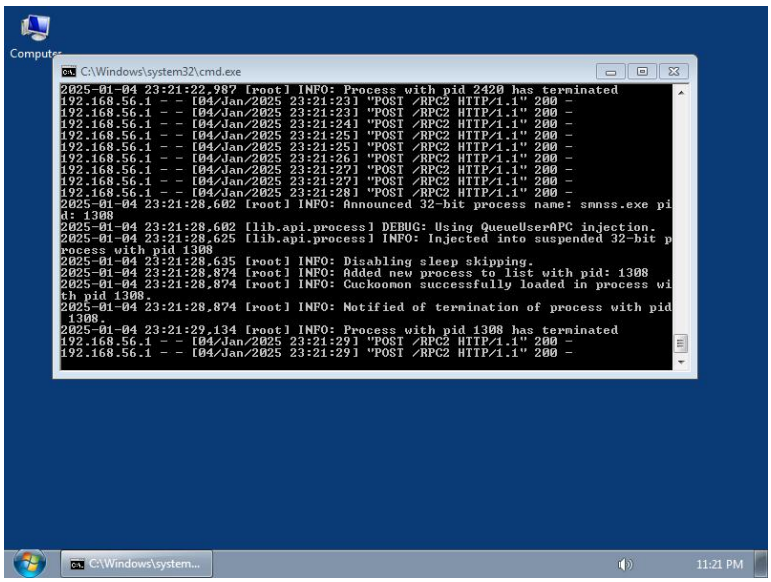

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:44,338 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2752
2025-01-04 23:21:44,338 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:44,378 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2752
2025-01-04 23:21:44,391 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:44,391 [root] INFO: Added new process to list with pid: 2752
2025-01-04 23:21:44,391 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2752.
2025-01-04 23:21:44,404 [root] INFO: Notified of termination of process with pid
 2752.
2025-01-04 23:21:44,693 [root] INFO: Process with pid 2752 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:47] "POST /RPC2 HTTP/1.1" 200 -
11:21 PM

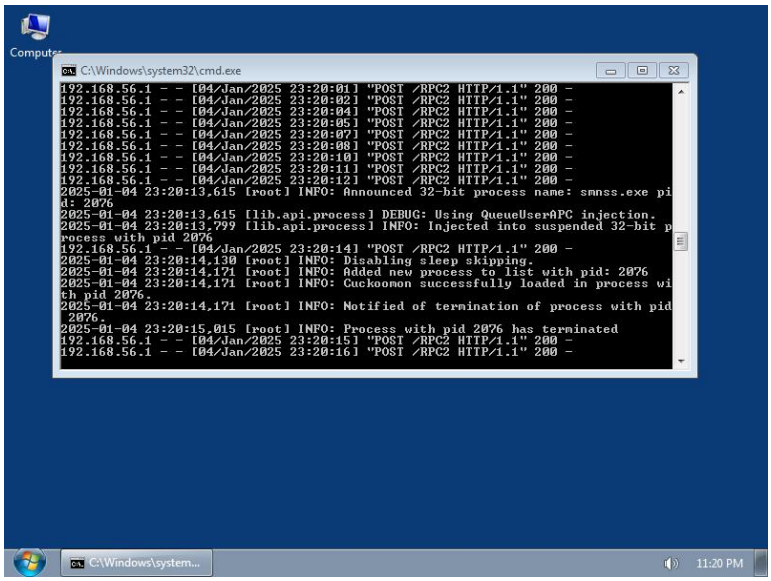

C:\Windows\system32\cmd.exe
th pid 2420.
2025-01-04 23:21:22,711 [root] INFO: Notified of termination of process with pid
 2420.
2025-01-04 23:21:22,987 [root] INFO: Process with pid 2420 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:28] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:28,602 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1308
2025-01-04 23:21:28,602 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:28,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1308
2025-01-04 23:21:28,635 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:28,874 [root] INFO: Added new process to list with pid: 1308
2025-01-04 23:21:28,874 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1308.
2025-01-04 23:21:28,874 [root] INFO: Notified of termination of process with pid
 1308.
11:21 PM

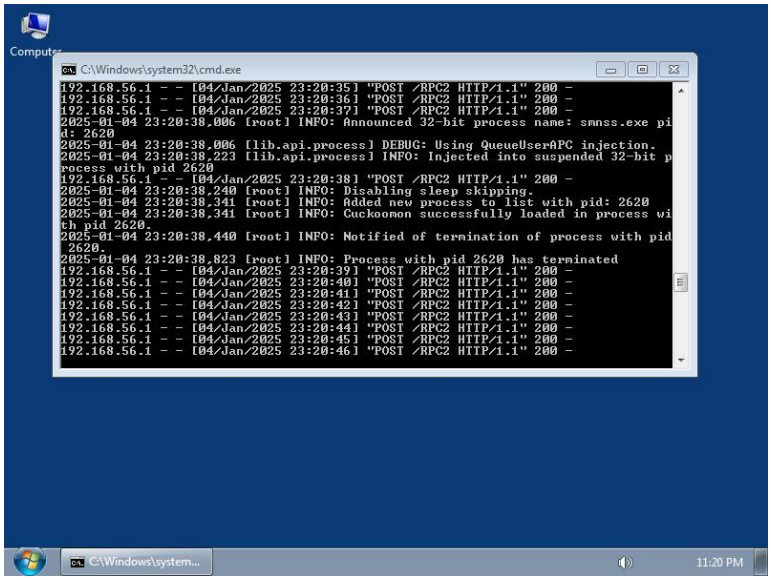

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:02] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,428 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 820
2025-01-04 23:22:03,428 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:03,602 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 820
192.168.56.1 - - [04/Jan/2025 23:22:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,651 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:03,667 [root] INFO: Added new process to list with pid: 820
2025-01-04 23:22:03,667 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 820.
2025-01-04 23:22:03,667 [root] INFO: Notified of termination of process with pid
 820.
2025-01-04 23:22:04,476 [root] INFO: Process with pid 820 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:07] "POST /RPC2 HTTP/1.1" 200 -
11:22 PM

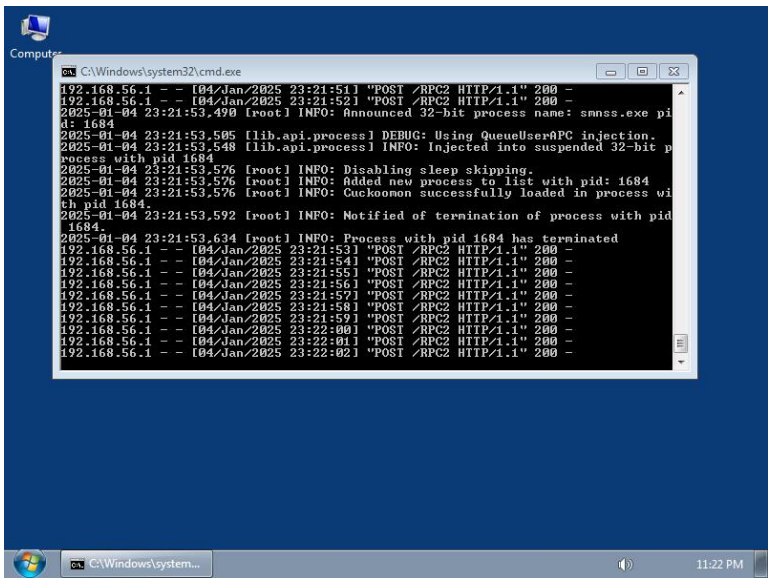

Computer
C:\Windows\system32\cmd.exe
820.
2025-01-04 23:22:04,476 [root] INFO: Process with pid 820 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:14,673 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 540
2025-01-04 23:22:14,690 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:14,707 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 540
2025-01-04 23:22:14,726 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:14,743 [root] INFO: Added new process to list with pid: 540
2025-01-04 23:22:14,743 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 540.
2025-01-04 23:22:14,743 [root] INFO: Notified of termination of process with pid
540.
2025-01-04 23:22:15,371 [root] INFO: Process with pid 540 has terminated
C:\Windows\system...
11:22 PM

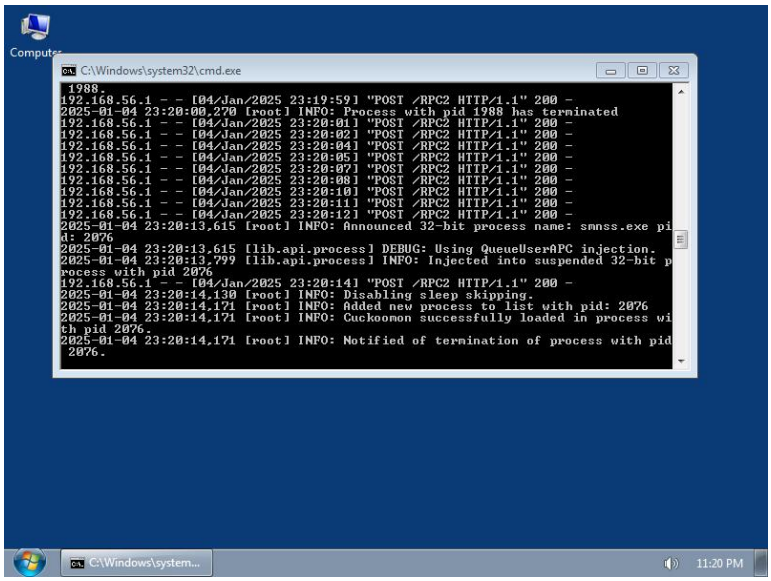

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:19:08,250 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:08,280 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2300
192.168.56.1 - - [04/Jan/2025 23:19:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:09] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:10,280 [lib.api.process] INFO: Successfully resumed process wit
h pid 2300
2025-01-04 23:19:10,296 [root] INFO: Added new process to list with pid: 2300
2025-01-04 23:19:10,312 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2300.
2025-01-04 23:19:10,312 [root] INFO: Added new file to list with path: C:\Window
s\System32\ctfmen.exe
2025-01-04 23:19:10,312 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:10,437 [root] INFO: Added new file to list with path: C:\Window
s\System32\shervans.dll
2025-01-04 23:19:10,437 [root] INFO: Added new file to list with path: C:\Window
s\System32\grcopy.dll
2025-01-04 23:19:10,687 [root] INFO: Added new file to list with path: C:\Window
s\System32\smnss.exe
2025-01-04 23:19:10,687 [root] INFO: Added new file to list with path: C:\Window
s\System32\satornas.dll
192.168.56.1 - - [04/Jan/2025 23:19:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:12] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

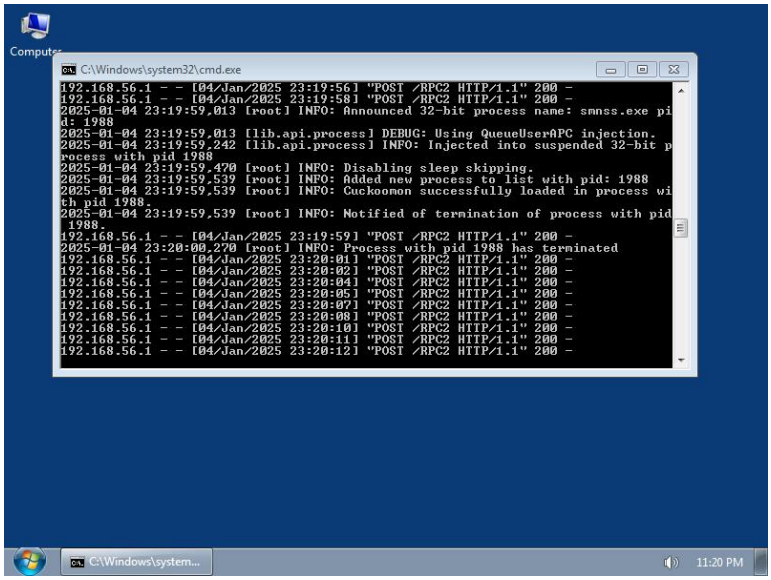

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:21:22,987 [root] INFO: Process with pid 2420 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:28] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:28,602 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1308
2025-01-04 23:21:28,602 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:28,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1308
2025-01-04 23:21:28,635 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:28,874 [root] INFO: Added new process to list with pid: 1308
2025-01-04 23:21:28,874 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1308.
2025-01-04 23:21:28,874 [root] INFO: Notified of termination of process with pid
1308.
2025-01-04 23:21:29,134 [root] INFO: Process with pid 1308 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

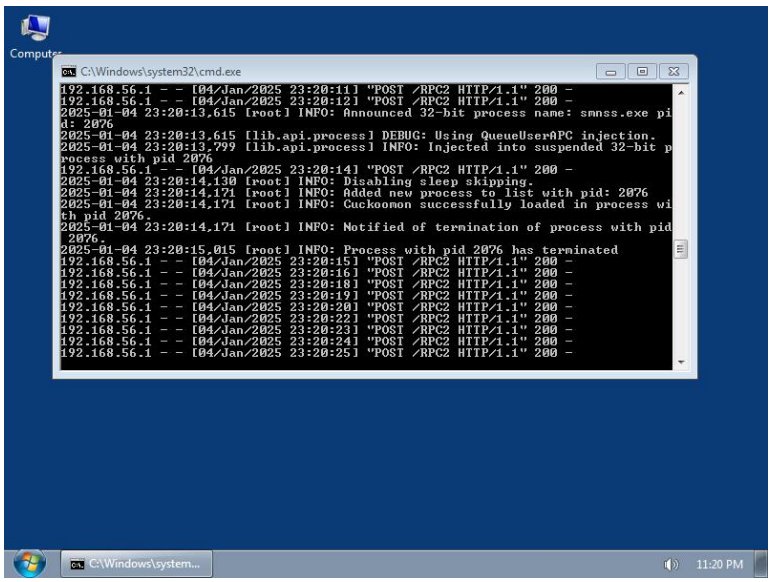

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:12] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:13,615 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2076
2025-01-04 23:20:13,615 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:13,799 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2076
192.168.56.1 - - [04/Jan/2025 23:20:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:14,130 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:14,171 [root] INFO: Added new process to list with pid: 2076
2025-01-04 23:20:14,171 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2076.
2025-01-04 23:20:14,171 [root] INFO: Notified of termination of process with pid
 2076.
2025-01-04 23:20:15,015 [root] INFO: Process with pid 2076 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:16] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

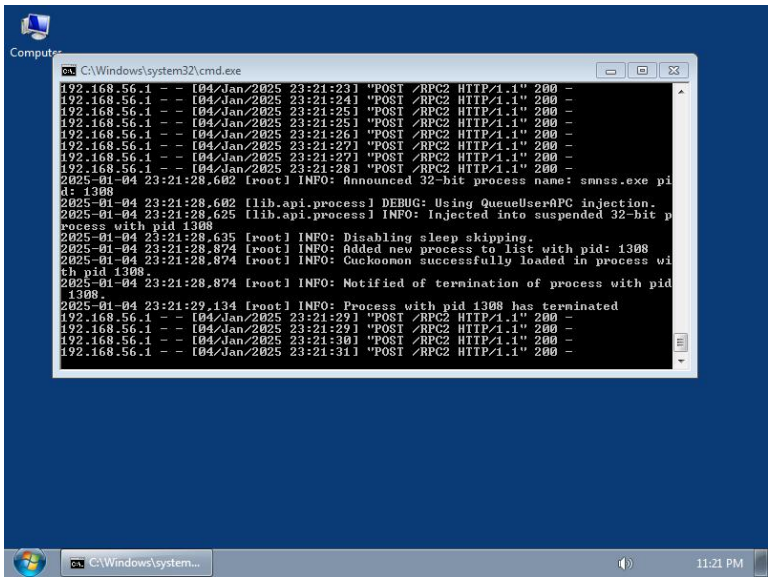

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:37] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,006 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2620
2025-01-04 23:20:38,006 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:38,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2620
192.168.56.1 - - [04/Jan/2025 23:20:38] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,240 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:38,341 [root] INFO: Added new process to list with pid: 2620
2025-01-04 23:20:38,341 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2620.
2025-01-04 23:20:38,440 [root] INFO: Notified of termination of process with pid
 2620.
2025-01-04 23:20:38,823 [root] INFO: Process with pid 2620 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:46] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

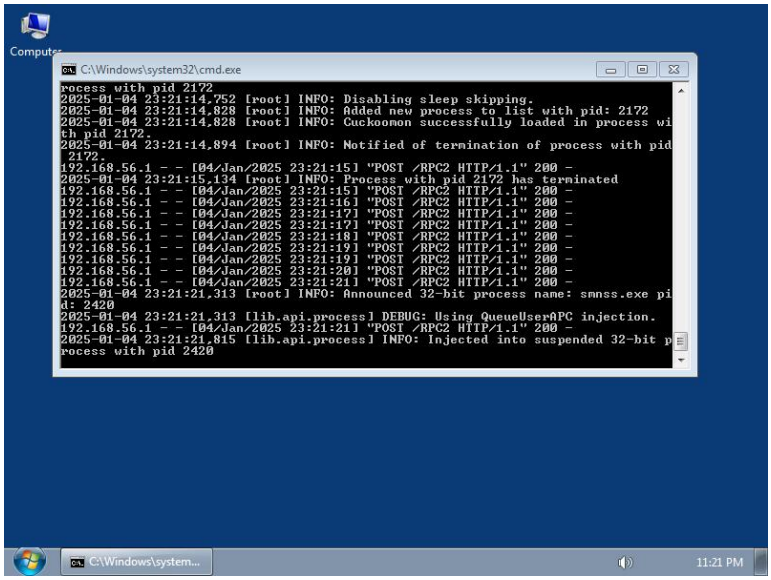

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:52] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:53,490 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1684
2025-01-04 23:21:53,505 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:53,548 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1684
2025-01-04 23:21:53,576 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:53,576 [root] INFO: Added new process to list with pid: 1684
2025-01-04 23:21:53,576 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1684.
2025-01-04 23:21:53,592 [root] INFO: Notified of termination of process with pid
 1684.
2025-01-04 23:21:53,634 [root] INFO: Process with pid 1684 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:02] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

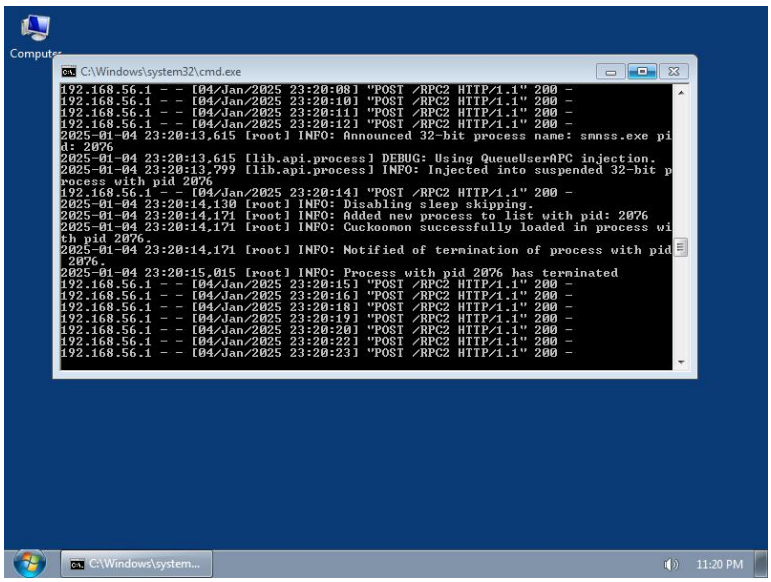

Computer
C:\Windows\system32\cmd.exe
1988.
192.168.56.1 - - [04/Jan/2025 23:19:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:00,270 [root] INFO: Process with pid 1988 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:12] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:13,615 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2076
2025-01-04 23:20:13,615 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:13,799 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2076
192.168.56.1 - - [04/Jan/2025 23:20:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:14,130 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:14,171 [root] INFO: Added new process to list with pid: 2076
2025-01-04 23:20:14,171 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2076.
2025-01-04 23:20:14,171 [root] INFO: Notified of termination of process with pid
2076.
C:\Windows\system...
11:20 PM

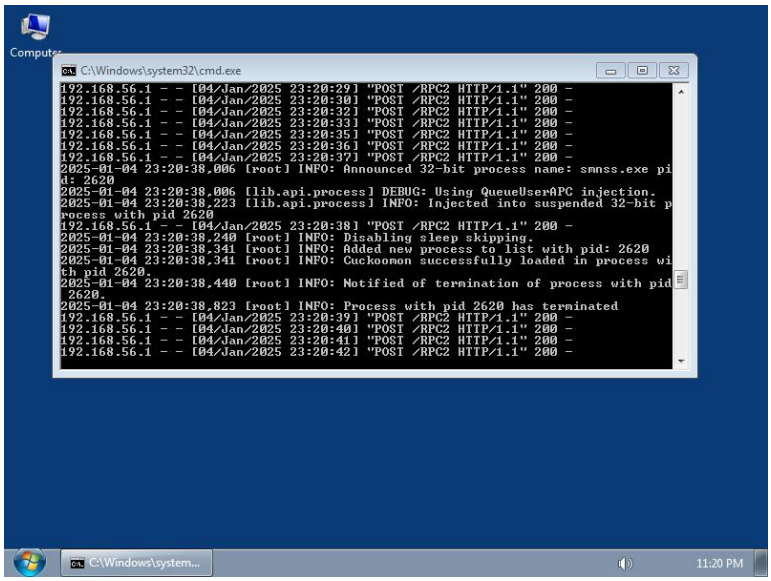

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:59,013 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1988
2025-01-04 23:19:59,013 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:59,242 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1988
2025-01-04 23:19:59,470 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:59,539 [root] INFO: Added new process to list with pid: 1988
2025-01-04 23:19:59,539 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1988.
2025-01-04 23:19:59,539 [root] INFO: Notified of termination of process with pid
1988.
192.168.56.1 - - [04/Jan/2025 23:19:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:00,270 [root] INFO: Process with pid 1988 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:12] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

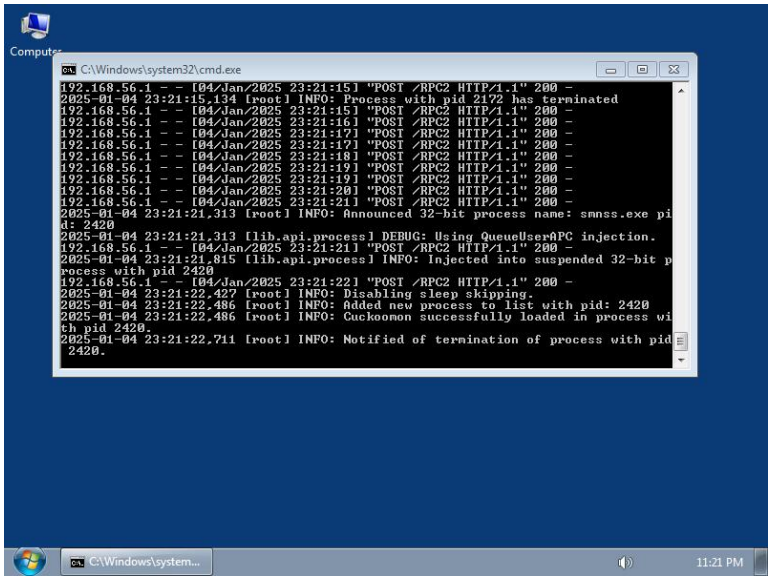

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:12] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:13,615 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2076
2025-01-04 23:20:13,615 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:13,799 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2076
192.168.56.1 - - [04/Jan/2025 23:20:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:14,130 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:14,171 [root] INFO: Added new process to list with pid: 2076
2025-01-04 23:20:14,171 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2076.
2025-01-04 23:20:14,171 [root] INFO: Notified of termination of process with pid
2076.
2025-01-04 23:20:15,015 [root] INFO: Process with pid 2076 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:25] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

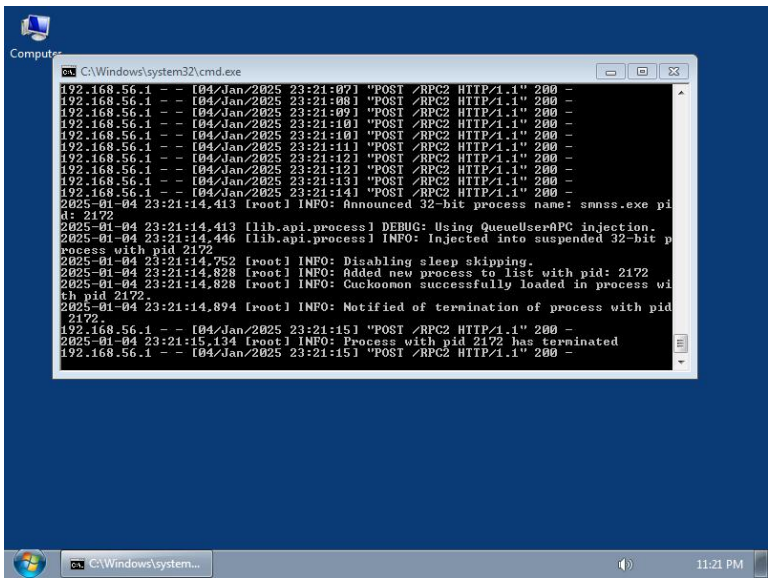

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:28] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:28,602 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1308
2025-01-04 23:21:28,602 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:28,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1308
2025-01-04 23:21:28,635 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:28,874 [root] INFO: Added new process to list with pid: 1308
2025-01-04 23:21:28,874 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1308.
2025-01-04 23:21:28,874 [root] INFO: Notified of termination of process with pid
 1308.
2025-01-04 23:21:29,134 [root] INFO: Process with pid 1308 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:31] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

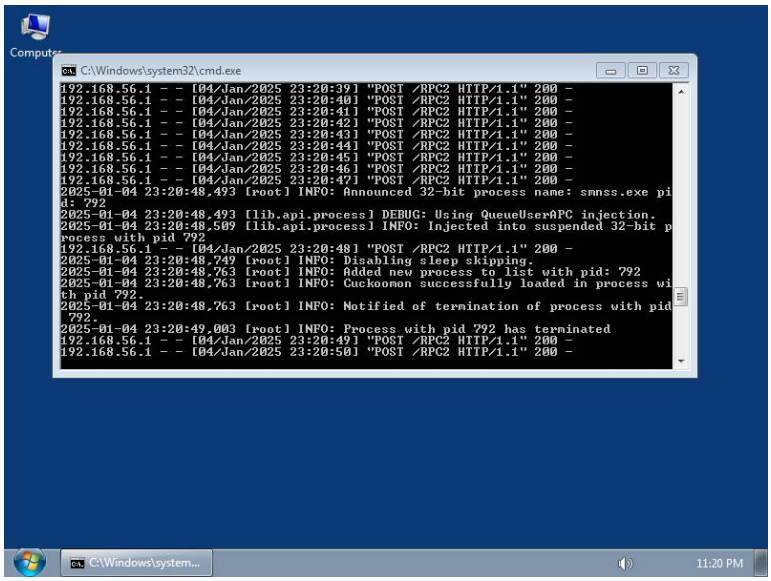

C:\Windows\system32\cmd.exe
rocess with pid 2172
2025-01-04 23:21:14,752 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:14,828 [root] INFO: Added new process to list with pid: 2172
2025-01-04 23:21:14,828 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2172.
2025-01-04 23:21:14,894 [root] INFO: Notified of termination of process with pid
 2172.
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:15,134 [root] INFO: Process with pid 2172 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,313 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2420
2025-01-04 23:21:21,313 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,815 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2420
C:\Windows\system...
11:21 PM

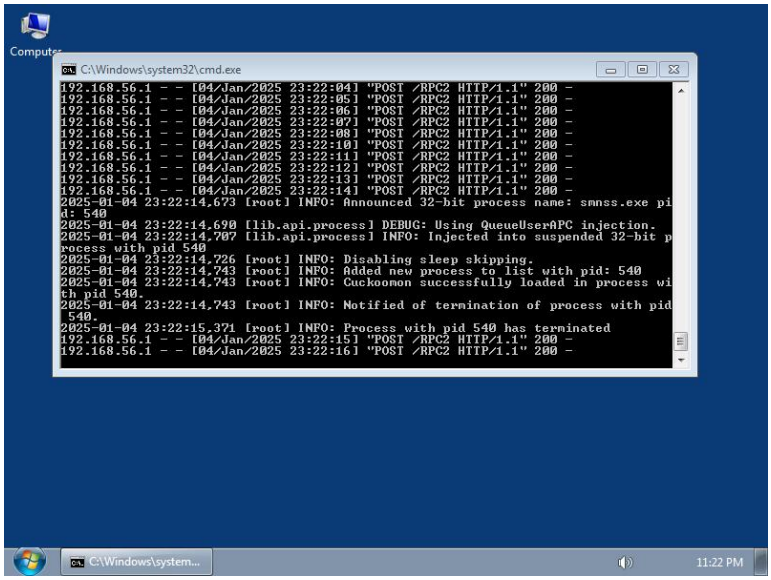

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:12] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:13,615 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2076
2025-01-04 23:20:13,615 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:13,799 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2076
192.168.56.1 - - [04/Jan/2025 23:20:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:14,130 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:14,171 [root] INFO: Added new process to list with pid: 2076
2025-01-04 23:20:14,171 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2076.
2025-01-04 23:20:14,171 [root] INFO: Notified of termination of process with pid
 2076.
2025-01-04 23:20:15,015 [root] INFO: Process with pid 2076 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:23] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

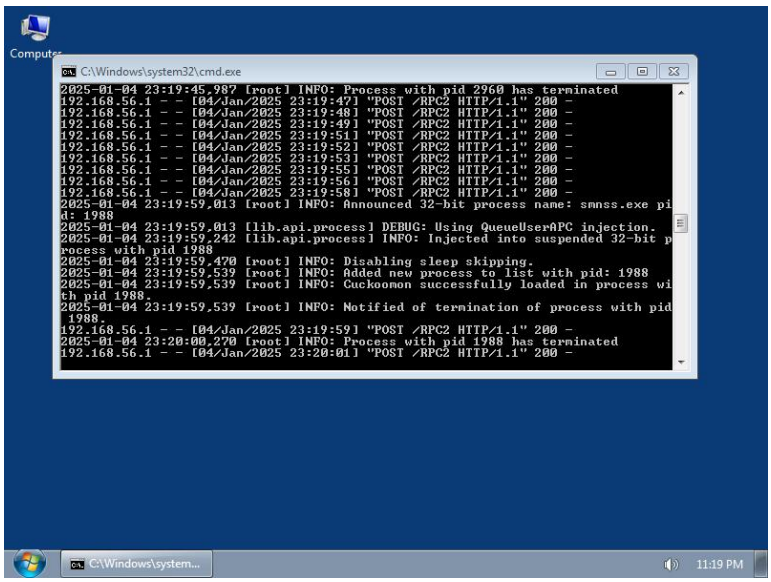

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:37] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,006 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2620
2025-01-04 23:20:38,006 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:38,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2620
192.168.56.1 - - [04/Jan/2025 23:20:38] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,240 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:38,341 [root] INFO: Added new process to list with pid: 2620
2025-01-04 23:20:38,341 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2620.
2025-01-04 23:20:38,440 [root] INFO: Notified of termination of process with pid
2620.
2025-01-04 23:20:38,823 [root] INFO: Process with pid 2620 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:42] "POST /RPC2 HTTP/1.1" 200 -
Computer
C:\Windows\system...
11:20 PM

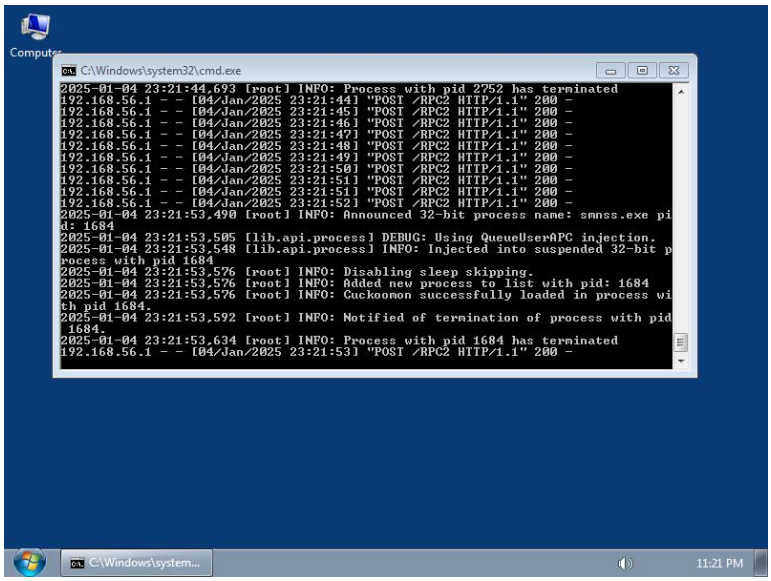

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:15,134 [root] INFO: Process with pid 2172 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,313 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2420
2025-01-04 23:21:21,313 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,815 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2420
192.168.56.1 - - [04/Jan/2025 23:21:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:22,427 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:22,486 [root] INFO: Added new process to list with pid: 2420
2025-01-04 23:21:22,486 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2420.
2025-01-04 23:21:22,711 [root] INFO: Notified of termination of process with pid
2420.
Computer
C:\Windows\system...
11:21 PM

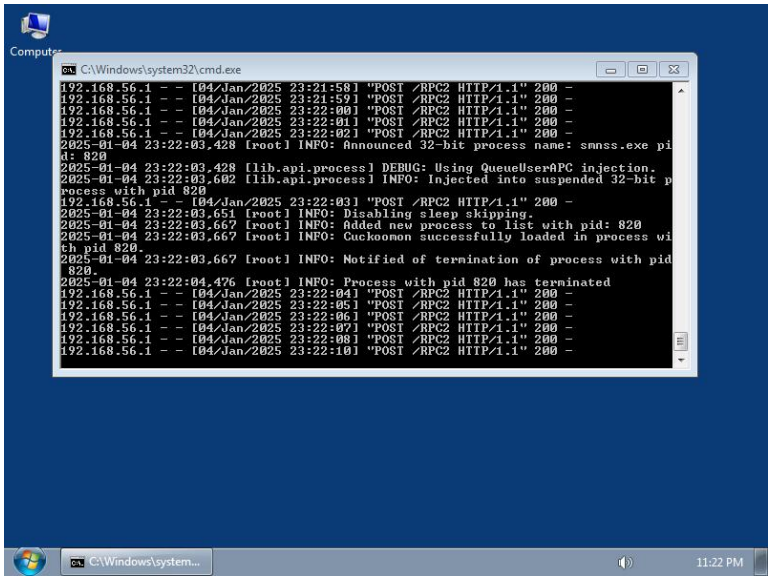

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:14,413 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2172
2025-01-04 23:21:14,413 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:14,446 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2172
2025-01-04 23:21:14,752 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:14,828 [root] INFO: Added new process to list with pid: 2172
2025-01-04 23:21:14,828 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2172.
2025-01-04 23:21:14,894 [root] INFO: Notified of termination of process with pid
2172.
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:15,134 [root] INFO: Process with pid 2172 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
Computer
C:\Windows\system...
11:21 PM

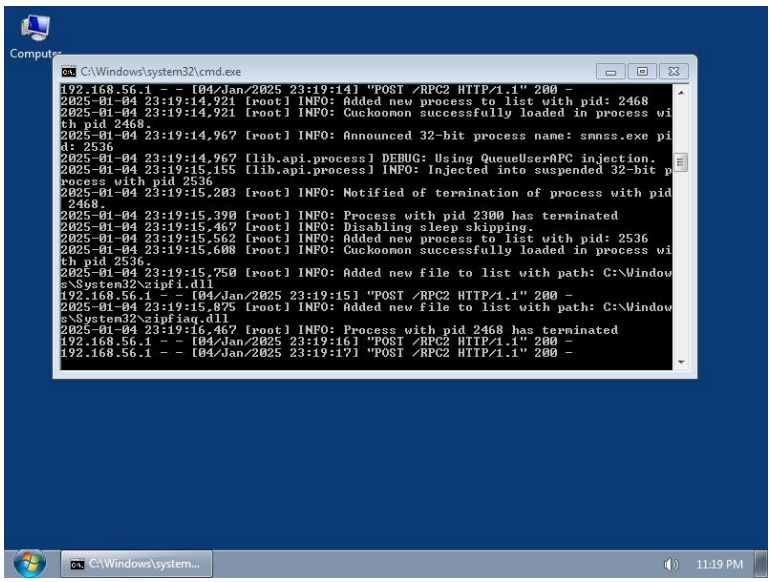

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:47] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,493 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 792
2025-01-04 23:20:48,493 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:48,509 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 792
192.168.56.1 - - [04/Jan/2025 23:20:48] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,749 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:48,763 [root] INFO: Added new process to list with pid: 792
2025-01-04 23:20:48,763 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 792.
2025-01-04 23:20:48,763 [root] INFO: Notified of termination of process with pid
 792.
2025-01-04 23:20:49,003 [root] INFO: Process with pid 792 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:50] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

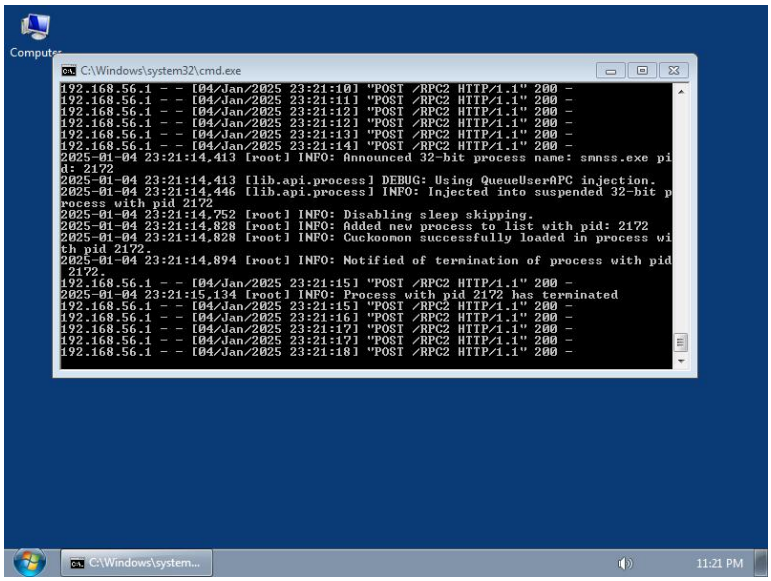

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:14,673 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 540
2025-01-04 23:22:14,690 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:14,707 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 540
2025-01-04 23:22:14,726 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:14,743 [root] INFO: Added new process to list with pid: 540
2025-01-04 23:22:14,743 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 540.
2025-01-04 23:22:14,743 [root] INFO: Notified of termination of process with pid
 540.
2025-01-04 23:22:15,371 [root] INFO: Process with pid 540 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:16] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

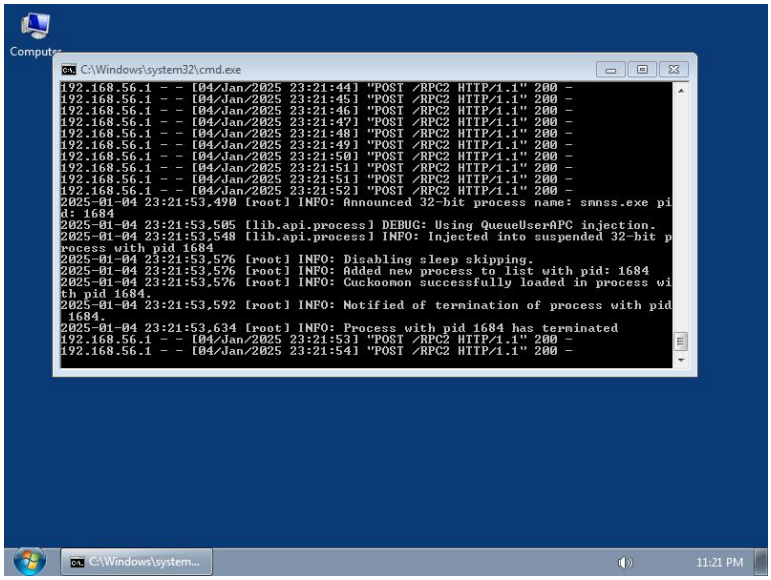

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:19:45,987 [root] INFO: Process with pid 2960 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:59,013 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1988
2025-01-04 23:19:59,013 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:59,242 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1988
2025-01-04 23:19:59,470 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:59,539 [root] INFO: Added new process to list with pid: 1988
2025-01-04 23:19:59,539 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1988.
2025-01-04 23:19:59,539 [root] INFO: Notified of termination of process with pid
 1988.
192.168.56.1 - - [04/Jan/2025 23:19:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:00,270 [root] INFO: Process with pid 1988 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:01] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

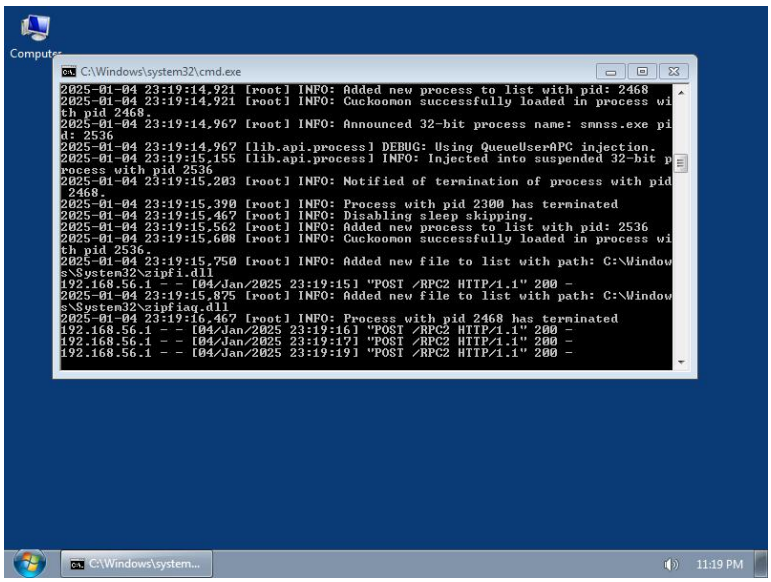

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:21:44,693 [root] INFO: Process with pid 2752 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:52] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:53,490 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1684
2025-01-04 23:21:53,505 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:53,548 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1684
2025-01-04 23:21:53,576 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:53,576 [root] INFO: Added new process to list with pid: 1684
2025-01-04 23:21:53,576 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1684.
2025-01-04 23:21:53,592 [root] INFO: Notified of termination of process with pid
 1684.
2025-01-04 23:21:53,634 [root] INFO: Process with pid 1684 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:53] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

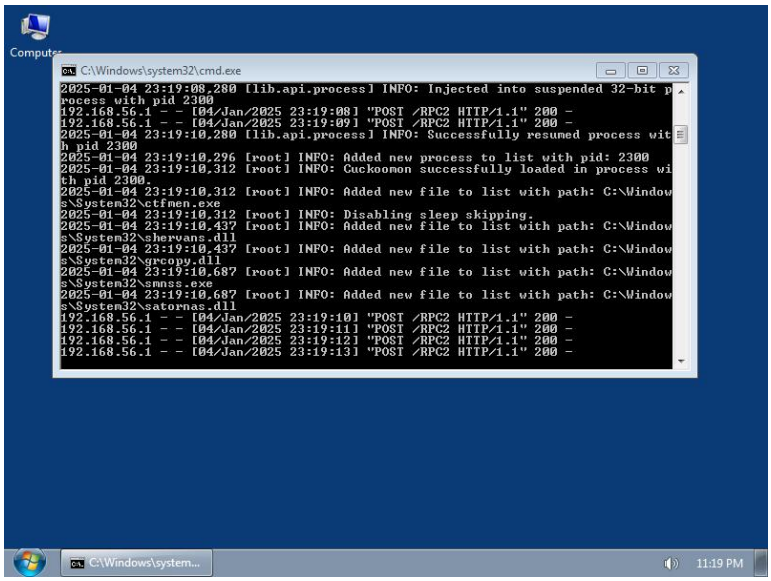

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:02] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,428 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 820
2025-01-04 23:22:03,428 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:03,602 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 820
192.168.56.1 - - [04/Jan/2025 23:22:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,651 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:03,667 [root] INFO: Added new process to list with pid: 820
2025-01-04 23:22:03,667 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 820.
2025-01-04 23:22:03,667 [root] INFO: Notified of termination of process with pid
 820.
2025-01-04 23:22:04,476 [root] INFO: Process with pid 820 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:10] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

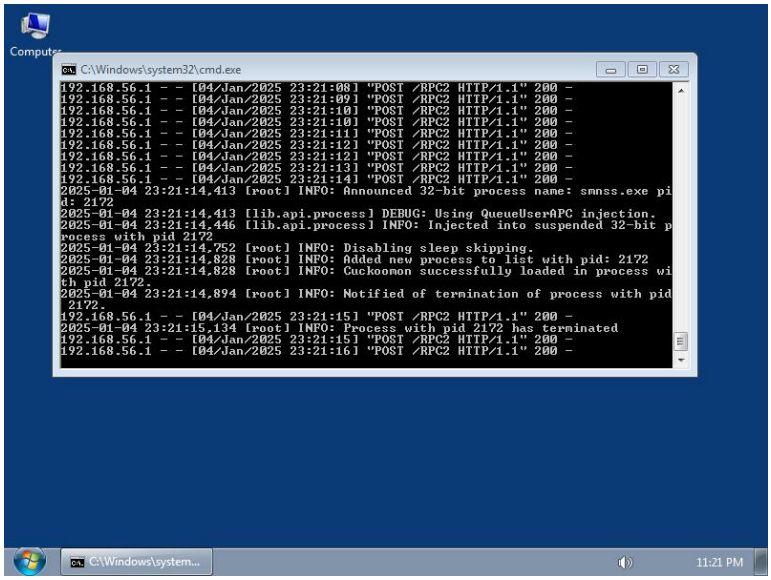

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:14,921 [root] INFO: Added new process to list with pid: 2468
2025-01-04 23:19:14,921 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2468.
2025-01-04 23:19:14,967 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2536
2025-01-04 23:19:14,967 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:15,155 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2536
2025-01-04 23:19:15,203 [root] INFO: Notified of termination of process with pid
 2468.
2025-01-04 23:19:15,390 [root] INFO: Process with pid 2300 has terminated
2025-01-04 23:19:15,467 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:15,562 [root] INFO: Added new process to list with pid: 2536
2025-01-04 23:19:15,608 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2536.
2025-01-04 23:19:15,750 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfi.dll
192.168.56.1 - - [04/Jan/2025 23:19:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:15,875 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfiaq.dll
2025-01-04 23:19:16,467 [root] INFO: Process with pid 2468 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:17] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

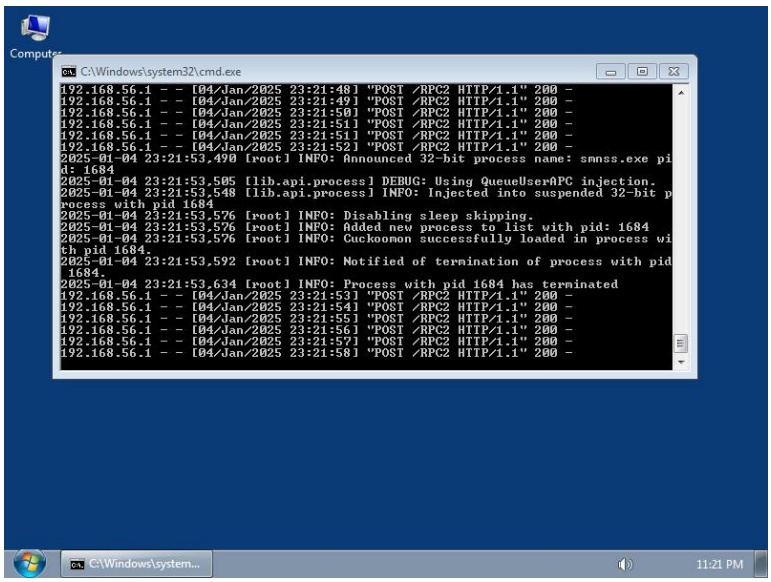

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:14,413 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2172
2025-01-04 23:21:14,413 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:14,446 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2172
2025-01-04 23:21:14,752 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:14,828 [root] INFO: Added new process to list with pid: 2172
2025-01-04 23:21:14,828 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2172.
2025-01-04 23:21:14,894 [root] INFO: Notified of termination of process with pid
 2172.
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:15,134 [root] INFO: Process with pid 2172 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:18] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

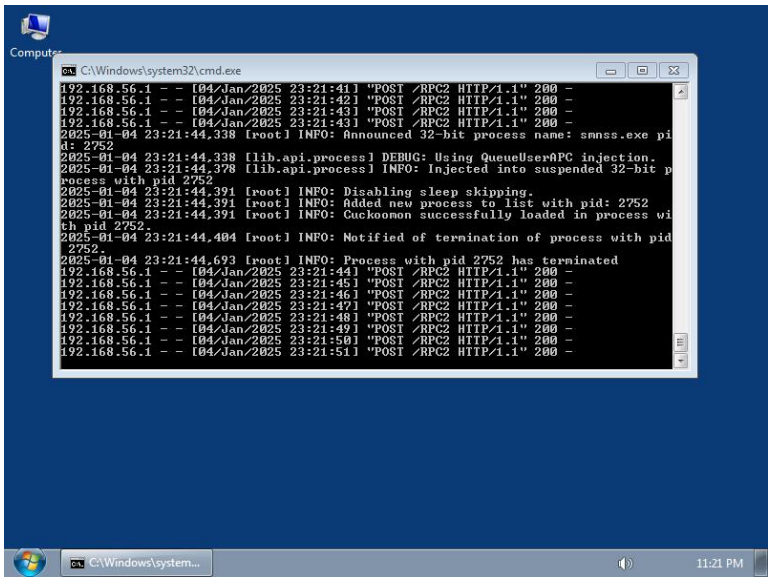

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:52] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:53,490 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1684
2025-01-04 23:21:53,505 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:53,548 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1684
2025-01-04 23:21:53,576 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:53,576 [root] INFO: Added new process to list with pid: 1684
2025-01-04 23:21:53,576 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1684.
2025-01-04 23:21:53,592 [root] INFO: Notified of termination of process with pid
 1684.
2025-01-04 23:21:53,634 [root] INFO: Process with pid 1684 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:54] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

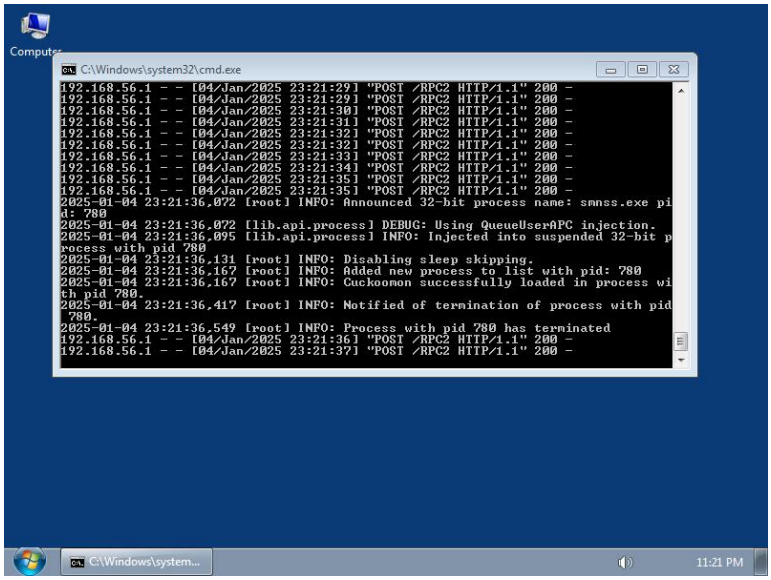

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:19:14,921 [root] INFO: Added new process to list with pid: 2468
2025-01-04 23:19:14,921 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2468.
2025-01-04 23:19:14,967 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2536
2025-01-04 23:19:14,967 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:15,155 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2536
2025-01-04 23:19:15,203 [root] INFO: Notified of termination of process with pid
 2468.
2025-01-04 23:19:15,390 [root] INFO: Process with pid 2300 has terminated
2025-01-04 23:19:15,467 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:15,562 [root] INFO: Added new process to list with pid: 2536
2025-01-04 23:19:15,608 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2536.
2025-01-04 23:19:15,750 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfi.dll
192.168.56.1 - - [04/Jan/2025 23:19:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:15,875 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfiaq.dll
2025-01-04 23:19:16,467 [root] INFO: Process with pid 2468 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:19] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

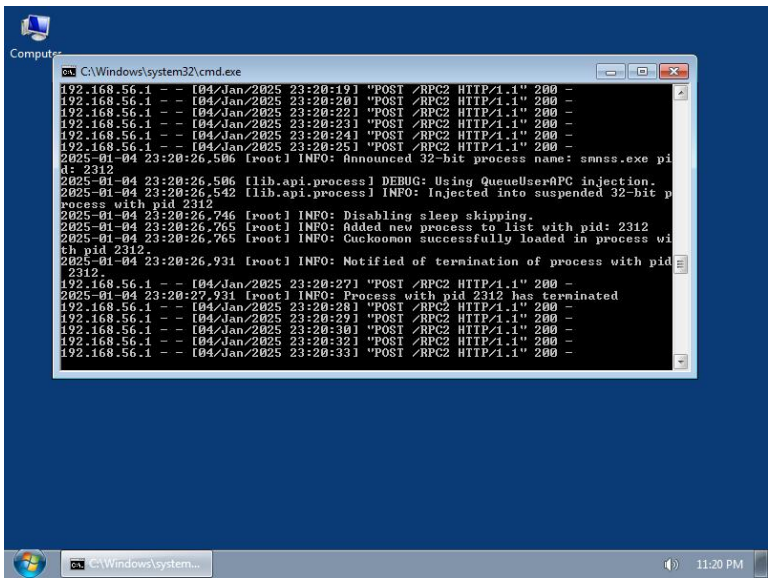

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:19:08,280 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2300
192.168.56.1 - - [04/Jan/2025 23:19:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:09] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:10,280 [lib.api.process] INFO: Successfully resumed process with pid 2300
2025-01-04 23:19:10,296 [root] INFO: Added new process to list with pid: 2300
2025-01-04 23:19:10,312 [root] INFO: Cuckoomon successfully loaded in process with pid 2300.
2025-01-04 23:19:10,312 [root] INFO: Added new file to list with path: C:\Windows\System32\ctfmen.exe
2025-01-04 23:19:10,312 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:10,437 [root] INFO: Added new file to list with path: C:\Windows\System32\shervans.dll
2025-01-04 23:19:10,437 [root] INFO: Added new file to list with path: C:\Windows\System32\qmcopy.dll
2025-01-04 23:19:10,687 [root] INFO: Added new file to list with path: C:\Windows\System32\smnss.exe
2025-01-04 23:19:10,687 [root] INFO: Added new file to list with path: C:\Windows\System32\satormas.dll
192.168.56.1 - - [04/Jan/2025 23:19:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:13] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

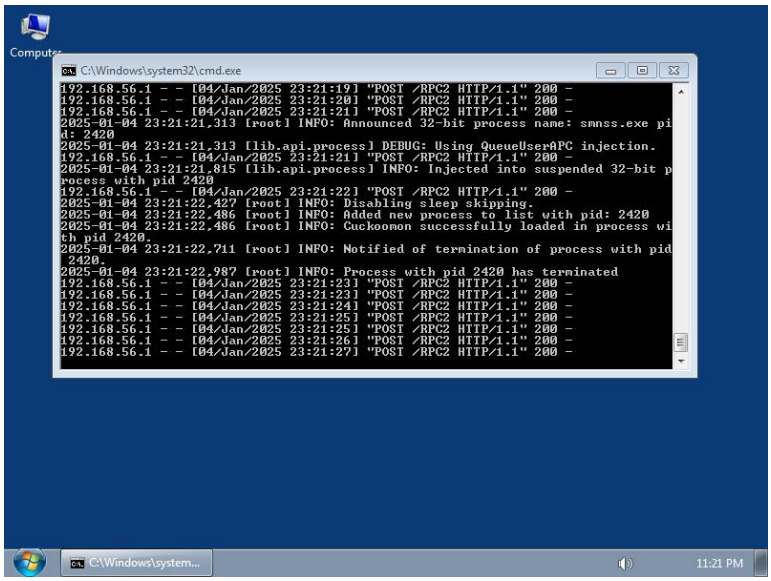

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:14,413 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2172
2025-01-04 23:21:14,413 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:14,446 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2172
2025-01-04 23:21:14,752 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:14,828 [root] INFO: Added new process to list with pid: 2172
2025-01-04 23:21:14,828 [root] INFO: Cuckoomon successfully loaded in process with pid 2172.
2025-01-04 23:21:14,894 [root] INFO: Notified of termination of process with pid 2172.
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:15,134 [root] INFO: Process with pid 2172 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:16] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

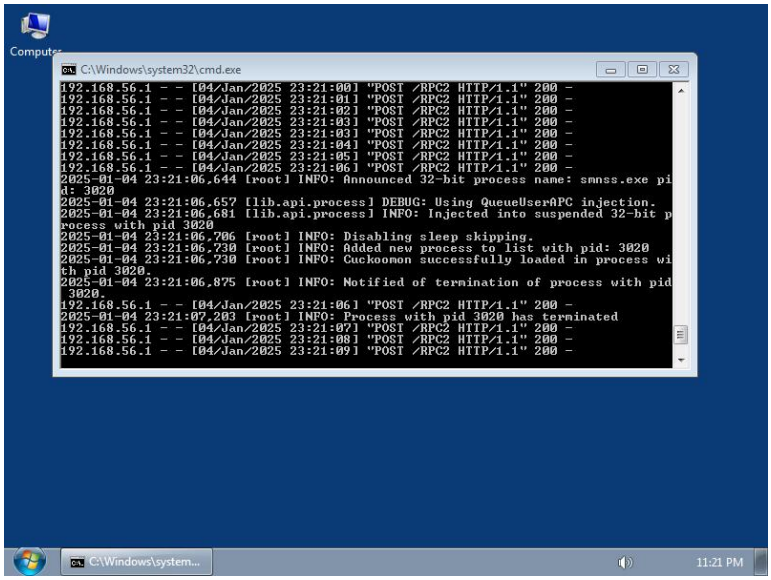

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:52] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:53,490 [root] INFO: Announced 32-bit process name: smnss.exe pid: 1684
2025-01-04 23:21:53,505 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:53,548 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 1684
2025-01-04 23:21:53,576 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:53,576 [root] INFO: Added new process to list with pid: 1684
2025-01-04 23:21:53,576 [root] INFO: Cuckoomon successfully loaded in process with pid 1684.
2025-01-04 23:21:53,592 [root] INFO: Notified of termination of process with pid 1684.
2025-01-04 23:21:53,634 [root] INFO: Process with pid 1684 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:58] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

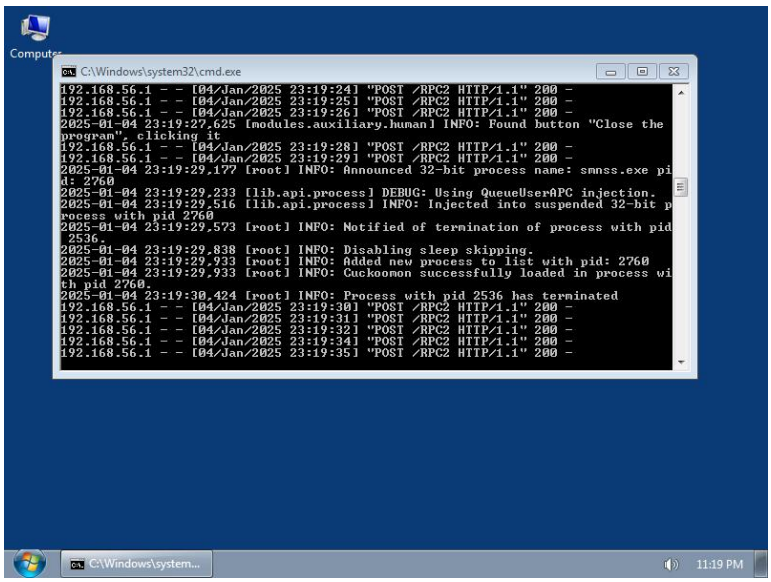

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:44,338 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2752
2025-01-04 23:21:44,338 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:44,378 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2752
2025-01-04 23:21:44,391 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:44,391 [root] INFO: Added new process to list with pid: 2752
2025-01-04 23:21:44,391 [root] INFO: Cuckoomon successfully loaded in process with pid 2752.
2025-01-04 23:21:44,404 [root] INFO: Notified of termination of process with pid 2752.
2025-01-04 23:21:44,693 [root] INFO: Process with pid 2752 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
11:21 PM

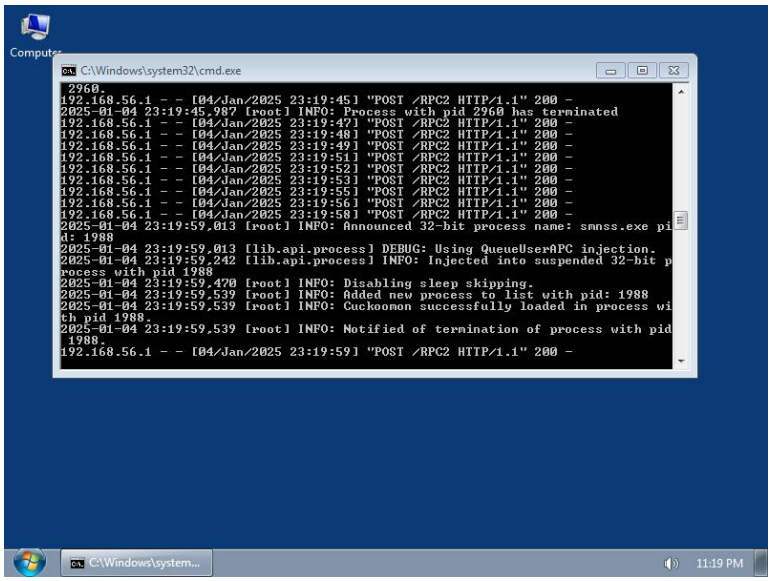

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:36,072 [root] INFO: Announced 32-bit process name: smnss.exe pid: 780
2025-01-04 23:21:36,072 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:36,095 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 780
2025-01-04 23:21:36,131 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:36,167 [root] INFO: Added new process to list with pid: 780
2025-01-04 23:21:36,167 [root] INFO: Cuckoomon successfully loaded in process with pid 780.
2025-01-04 23:21:36,417 [root] INFO: Notified of termination of process with pid 780.
2025-01-04 23:21:36,549 [root] INFO: Process with pid 780 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:37] "POST /RPC2 HTTP/1.1" 200 -
11:21 PM

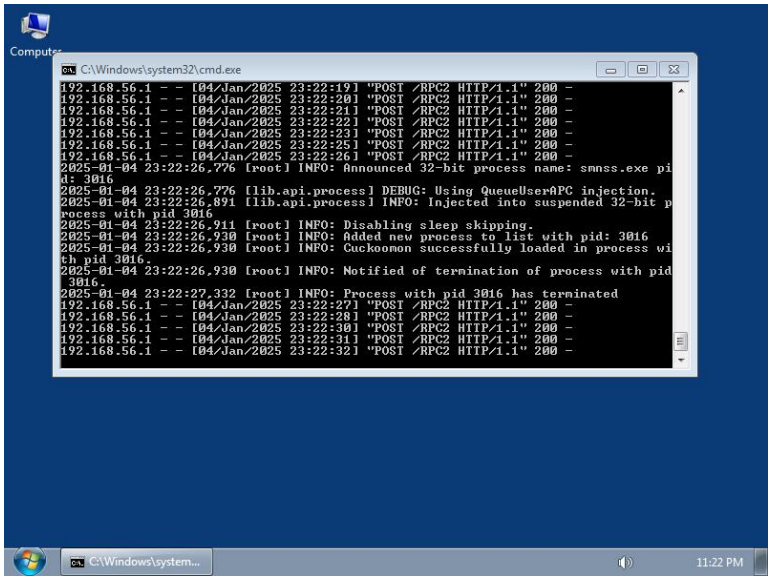

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:25] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:26,506 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2312
2025-01-04 23:20:26,506 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:26,542 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2312
2025-01-04 23:20:26,746 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:26,765 [root] INFO: Added new process to list with pid: 2312
2025-01-04 23:20:26,765 [root] INFO: Cuckoomon successfully loaded in process with pid 2312.
2025-01-04 23:20:26,931 [root] INFO: Notified of termination of process with pid 2312.
192.168.56.1 - - [04/Jan/2025 23:20:27] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:27,931 [root] INFO: Process with pid 2312 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:33] "POST /RPC2 HTTP/1.1" 200 -
11:20 PM

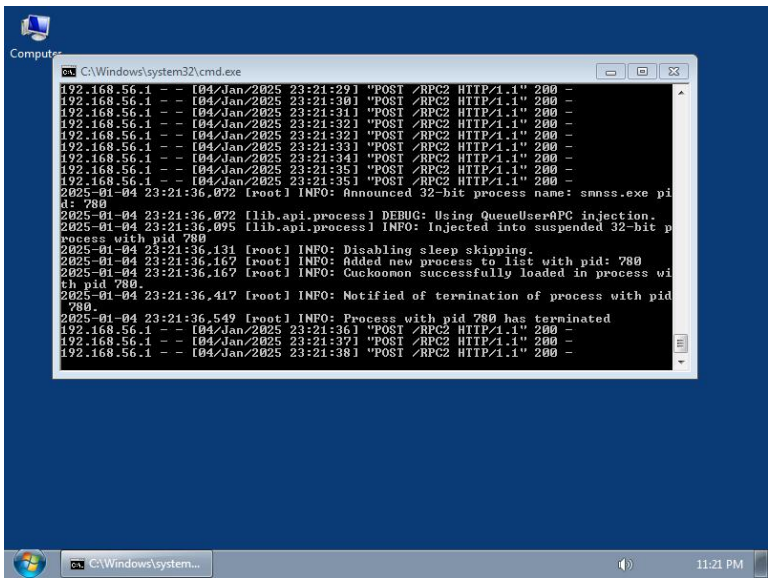

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,313 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2420
2025-01-04 23:21:21,313 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,815 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2420
192.168.56.1 - - [04/Jan/2025 23:21:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:22,427 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:22,486 [root] INFO: Added new process to list with pid: 2420
2025-01-04 23:21:22,486 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2420.
2025-01-04 23:21:22,711 [root] INFO: Notified of termination of process with pid
 2420.
2025-01-04 23:21:22,987 [root] INFO: Process with pid 2420 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

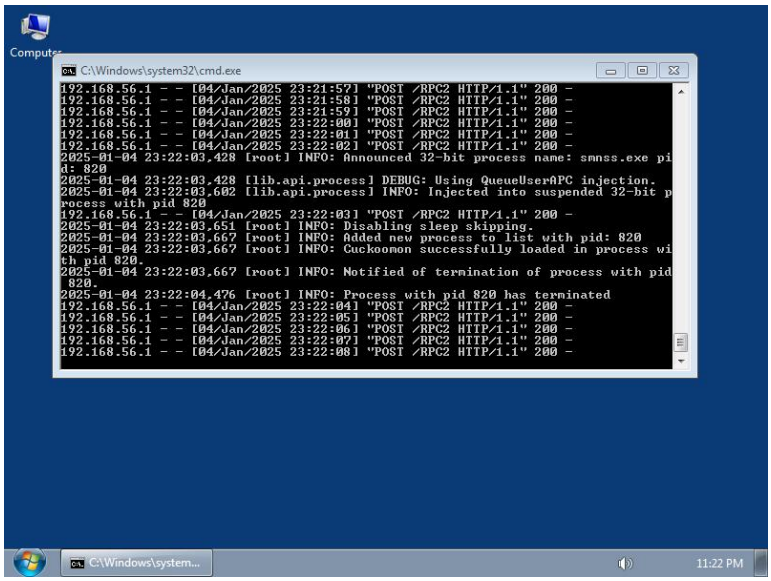

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:06,644 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3020
2025-01-04 23:21:06,657 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:06,681 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3020
2025-01-04 23:21:06,706 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:06,730 [root] INFO: Added new process to list with pid: 3020
2025-01-04 23:21:06,730 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3020.
2025-01-04 23:21:06,875 [root] INFO: Notified of termination of process with pid
 3020.
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:07,203 [root] INFO: Process with pid 3020 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:09] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

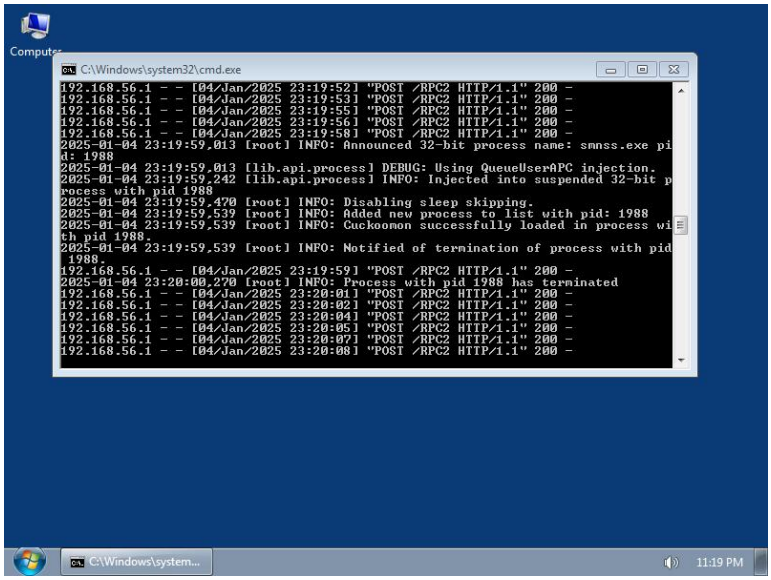

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:27,625 [modules.auxiliary.human] INFO: Found button "Close the
program", clicking it
192.168.56.1 - - [04/Jan/2025 23:19:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:29] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:29,177 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2760
2025-01-04 23:19:29,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:29,516 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2760
2025-01-04 23:19:29,573 [root] INFO: Notified of termination of process with pid
 2536.
2025-01-04 23:19:29,838 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:29,933 [root] INFO: Added new process to list with pid: 2760
2025-01-04 23:19:29,933 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2760.
2025-01-04 23:19:30,424 [root] INFO: Process with pid 2536 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:35] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

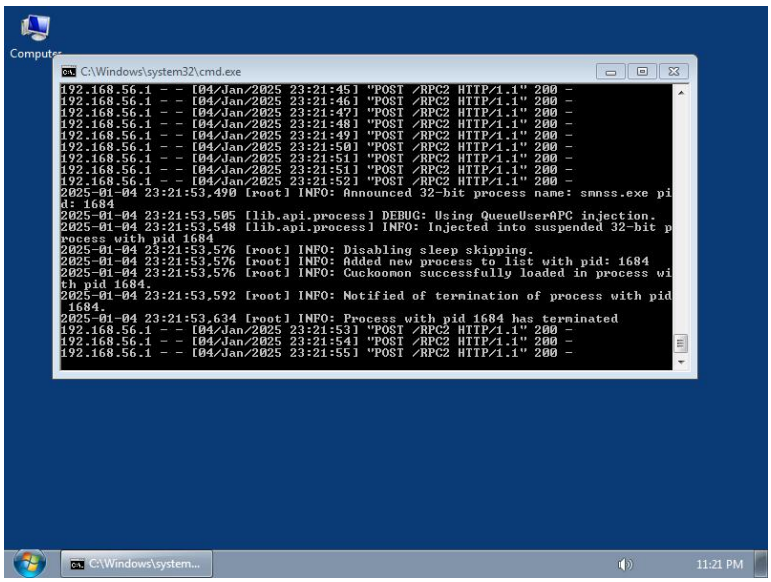

C:\Windows\system32\cmd.exe
2960.
192.168.56.1 - - [04/Jan/2025 23:19:45] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:45,987 [root] INFO: Process with pid 2960 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:59,013 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1988
2025-01-04 23:19:59,013 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:59,242 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1988
2025-01-04 23:19:59,470 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:59,539 [root] INFO: Added new process to list with pid: 1988
2025-01-04 23:19:59,539 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1988.
2025-01-04 23:19:59,539 [root] INFO: Notified of termination of process with pid
1988.
192.168.56.1 - - [04/Jan/2025 23:19:59] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

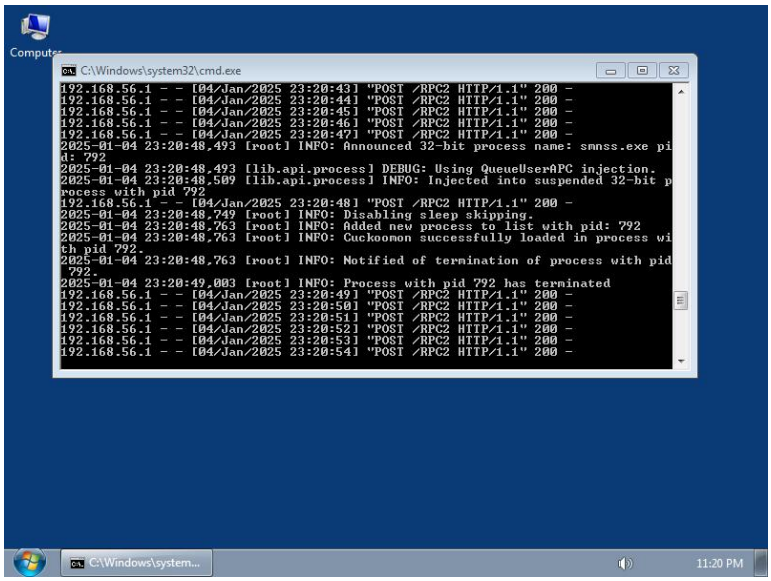

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:26,776 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3016
2025-01-04 23:22:26,776 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:26,891 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3016
2025-01-04 23:22:26,911 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:26,930 [root] INFO: Added new process to list with pid: 3016
2025-01-04 23:22:26,930 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3016.
2025-01-04 23:22:26,930 [root] INFO: Notified of termination of process with pid
3016.
2025-01-04 23:22:27,332 [root] INFO: Process with pid 3016 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:32] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

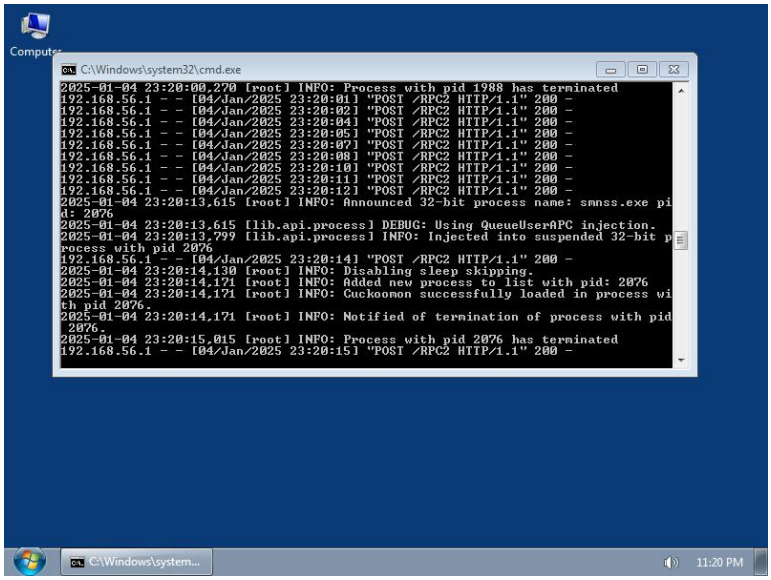

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:36,072 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 780
2025-01-04 23:21:36,072 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:36,095 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 780
2025-01-04 23:21:36,131 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:36,167 [root] INFO: Added new process to list with pid: 780
2025-01-04 23:21:36,167 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 780.
2025-01-04 23:21:36,417 [root] INFO: Notified of termination of process with pid
780.
2025-01-04 23:21:36,549 [root] INFO: Process with pid 780 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

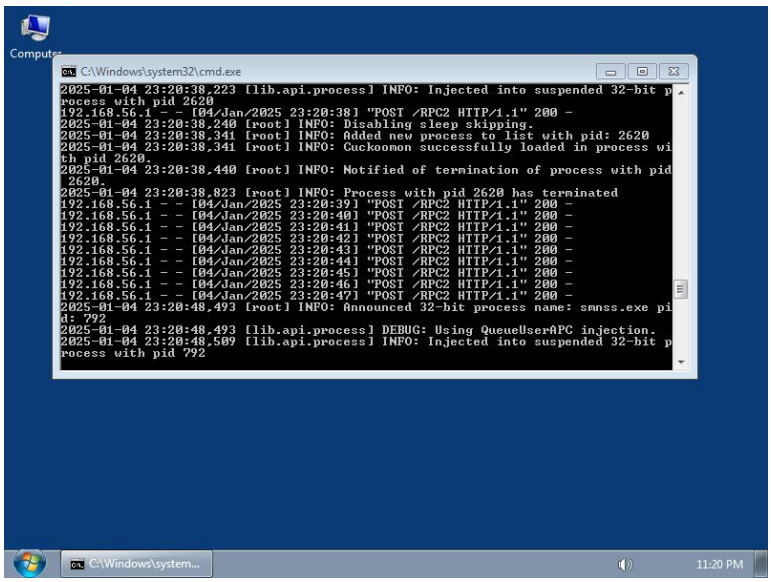

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:02] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,428 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 820
2025-01-04 23:22:03,428 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:03,602 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 820
192.168.56.1 - - [04/Jan/2025 23:22:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,651 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:03,667 [root] INFO: Added new process to list with pid: 820
2025-01-04 23:22:03,667 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 820.
2025-01-04 23:22:03,667 [root] INFO: Notified of termination of process with pid
 820.
2025-01-04 23:22:04,476 [root] INFO: Process with pid 820 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:08] "POST /RPC2 HTTP/1.1" 200 -
11:22 PM

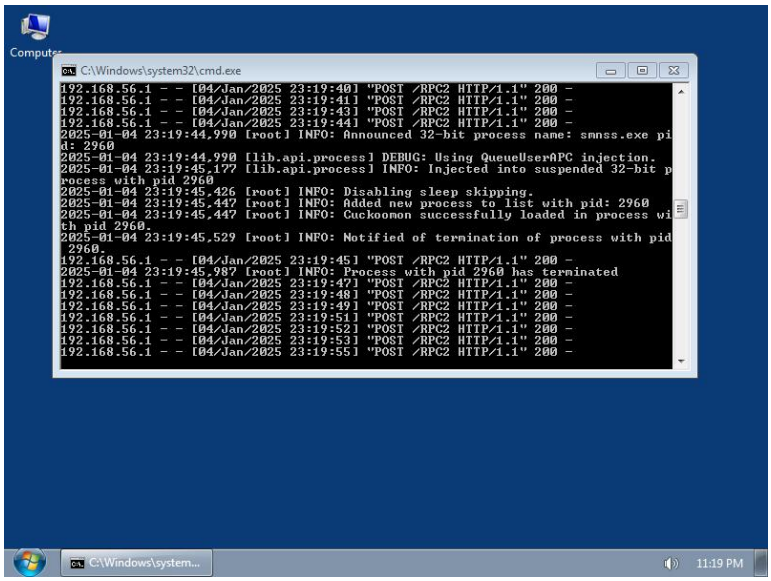

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:59,013 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1988
2025-01-04 23:19:59,013 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:59,242 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1988
2025-01-04 23:19:59,470 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:59,539 [root] INFO: Added new process to list with pid: 1988
2025-01-04 23:19:59,539 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1988.
2025-01-04 23:19:59,539 [root] INFO: Notified of termination of process with pid
 1988.
192.168.56.1 - - [04/Jan/2025 23:19:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:00,270 [root] INFO: Process with pid 1988 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:08] "POST /RPC2 HTTP/1.1" 200 -
11:19 PM

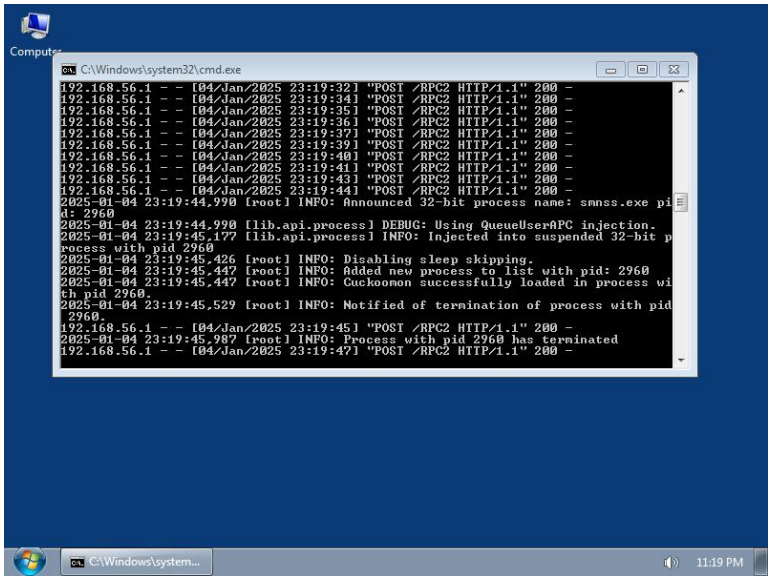

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:52] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:53,490 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1684
2025-01-04 23:21:53,505 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:53,548 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1684
2025-01-04 23:21:53,576 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:53,576 [root] INFO: Added new process to list with pid: 1684
2025-01-04 23:21:53,576 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1684.
2025-01-04 23:21:53,592 [root] INFO: Notified of termination of process with pid
 1684.
2025-01-04 23:21:53,634 [root] INFO: Process with pid 1684 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:55] "POST /RPC2 HTTP/1.1" 200 -
11:21 PM

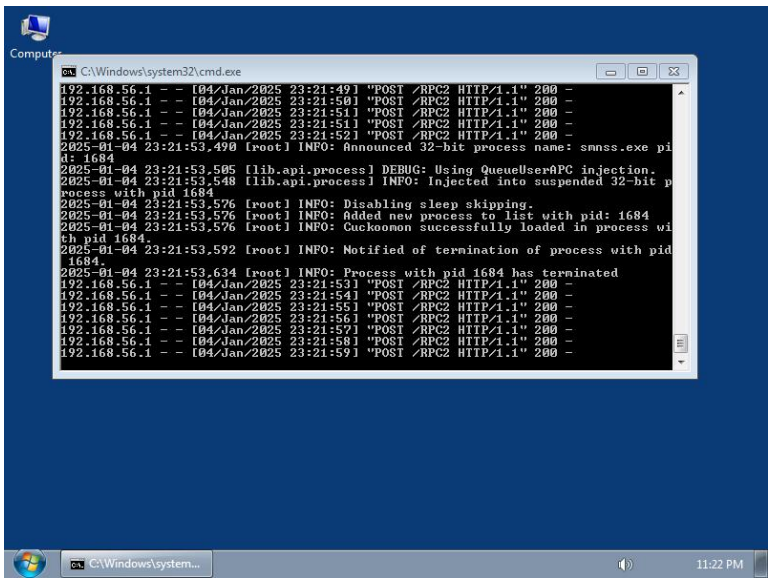

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:47] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,493 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 792
2025-01-04 23:20:48,493 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:48,509 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 792
192.168.56.1 - - [04/Jan/2025 23:20:48] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,749 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:48,763 [root] INFO: Added new process to list with pid: 792
2025-01-04 23:20:48,763 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 792.
2025-01-04 23:20:48,763 [root] INFO: Notified of termination of process with pid
 792.
2025-01-04 23:20:49,003 [root] INFO: Process with pid 792 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:54] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

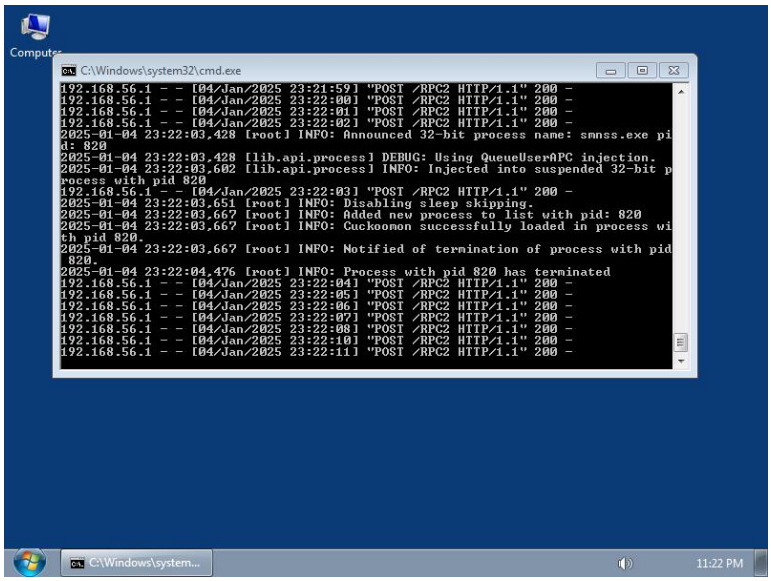

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:20:00,270 [root] INFO: Process with pid 1988 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:12] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:13,615 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2076
2025-01-04 23:20:13,615 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:13,799 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2076
192.168.56.1 - - [04/Jan/2025 23:20:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:14,130 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:14,171 [root] INFO: Added new process to list with pid: 2076
2025-01-04 23:20:14,171 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2076.
2025-01-04 23:20:14,171 [root] INFO: Notified of termination of process with pid
 2076.
2025-01-04 23:20:15,015 [root] INFO: Process with pid 2076 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:15] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

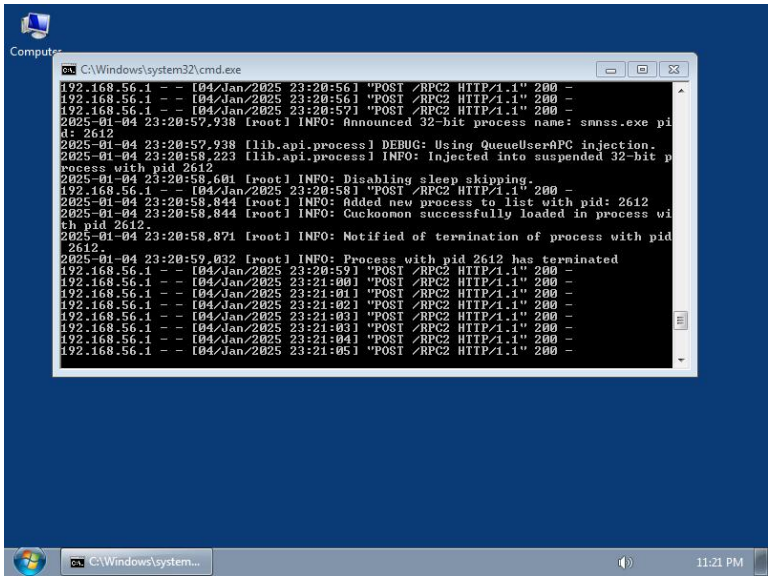

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:20:38,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2620
192.168.56.1 - - [04/Jan/2025 23:20:38] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,240 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:38,341 [root] INFO: Added new process to list with pid: 2620
2025-01-04 23:20:38,341 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2620.
2025-01-04 23:20:38,440 [root] INFO: Notified of termination of process with pid
 2620.
2025-01-04 23:20:38,823 [root] INFO: Process with pid 2620 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:47] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,493 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 792
2025-01-04 23:20:48,493 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:48,509 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 792
C:\Windows\system...
11:20 PM

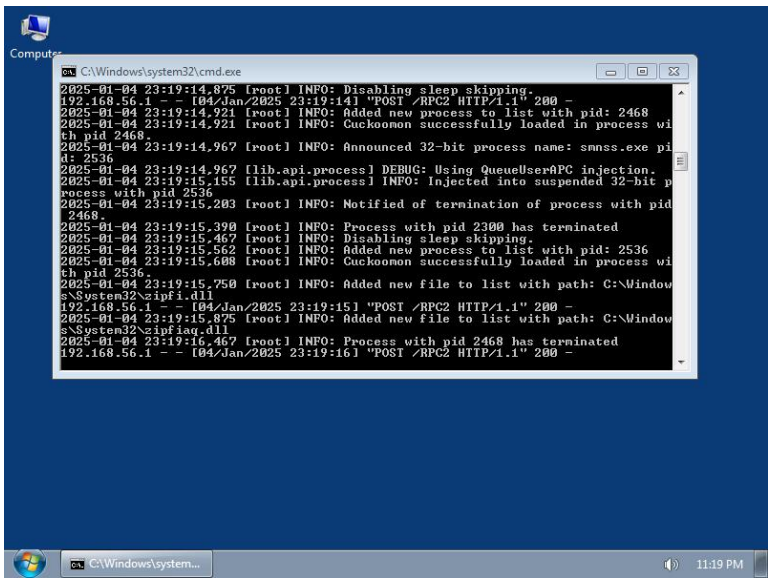

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:44] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:44,990 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2960
2025-01-04 23:19:44,990 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:45,177 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2960
2025-01-04 23:19:45,426 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:45,447 [root] INFO: Added new process to list with pid: 2960
2025-01-04 23:19:45,447 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2960.
2025-01-04 23:19:45,529 [root] INFO: Notified of termination of process with pid
 2960.
192.168.56.1 - - [04/Jan/2025 23:19:45] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:45,987 [root] INFO: Process with pid 2960 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:55] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

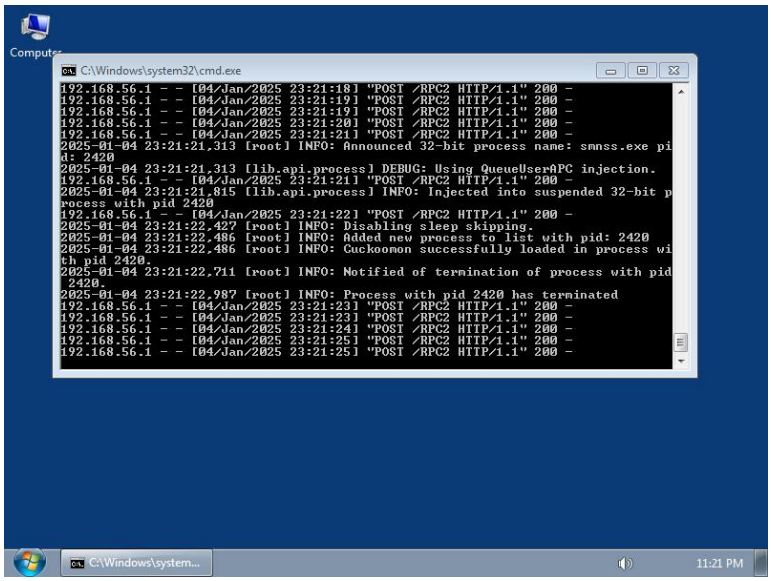

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:44] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:44,990 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2960
2025-01-04 23:19:44,990 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:45,177 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2960
2025-01-04 23:19:45,426 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:45,447 [root] INFO: Added new process to list with pid: 2960
2025-01-04 23:19:45,447 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2960.
2025-01-04 23:19:45,529 [root] INFO: Notified of termination of process with pid
 2960.
192.168.56.1 - - [04/Jan/2025 23:19:45] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:45,987 [root] INFO: Process with pid 2960 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:47] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

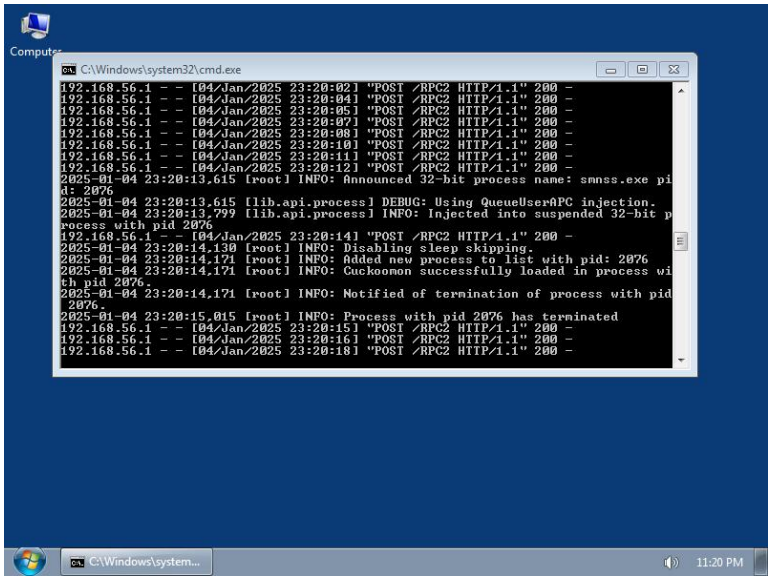

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:52] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:53,490 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1684
2025-01-04 23:21:53,505 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:53,548 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1684
2025-01-04 23:21:53,576 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:53,576 [root] INFO: Added new process to list with pid: 1684
2025-01-04 23:21:53,576 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1684.
2025-01-04 23:21:53,592 [root] INFO: Notified of termination of process with pid
 1684.
2025-01-04 23:21:53,634 [root] INFO: Process with pid 1684 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:59] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

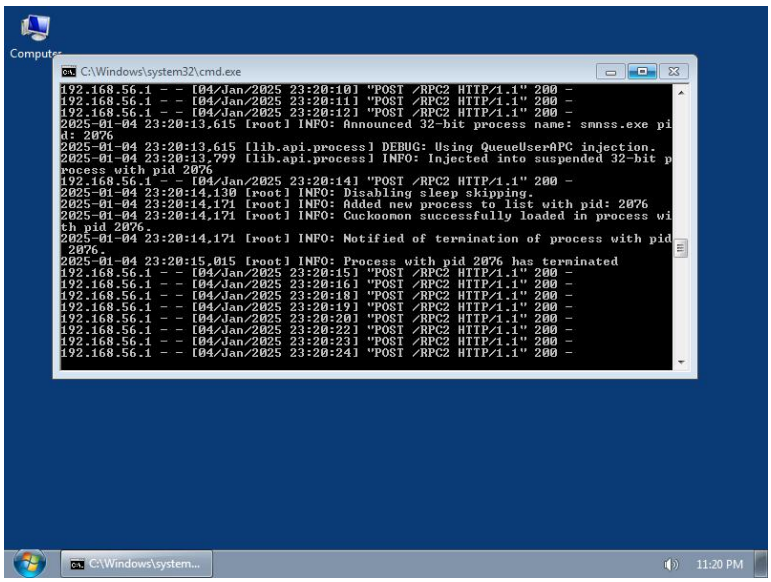

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:02] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,428 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 820
2025-01-04 23:22:03,428 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:03,602 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 820
192.168.56.1 - - [04/Jan/2025 23:22:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,651 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:03,667 [root] INFO: Added new process to list with pid: 820
2025-01-04 23:22:03,667 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 820.
2025-01-04 23:22:03,667 [root] INFO: Notified of termination of process with pid
 820.
2025-01-04 23:22:04,476 [root] INFO: Process with pid 820 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:11] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

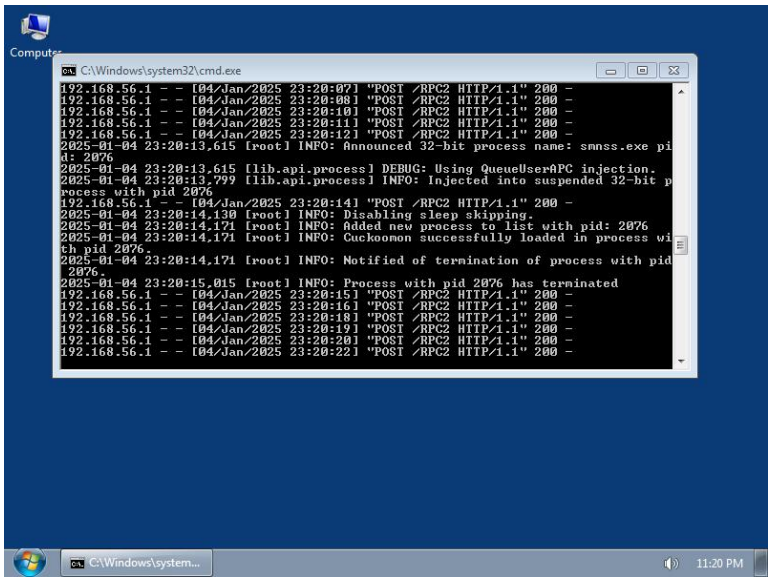

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:57] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:57,938 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2612
2025-01-04 23:20:57,938 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:58,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2612
2025-01-04 23:20:58,601 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [04/Jan/2025 23:20:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:58,844 [root] INFO: Added new process to list with pid: 2612
2025-01-04 23:20:58,844 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2612.
2025-01-04 23:20:58,871 [root] INFO: Notified of termination of process with pid
 2612.
2025-01-04 23:20:59,032 [root] INFO: Process with pid 2612 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:05] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

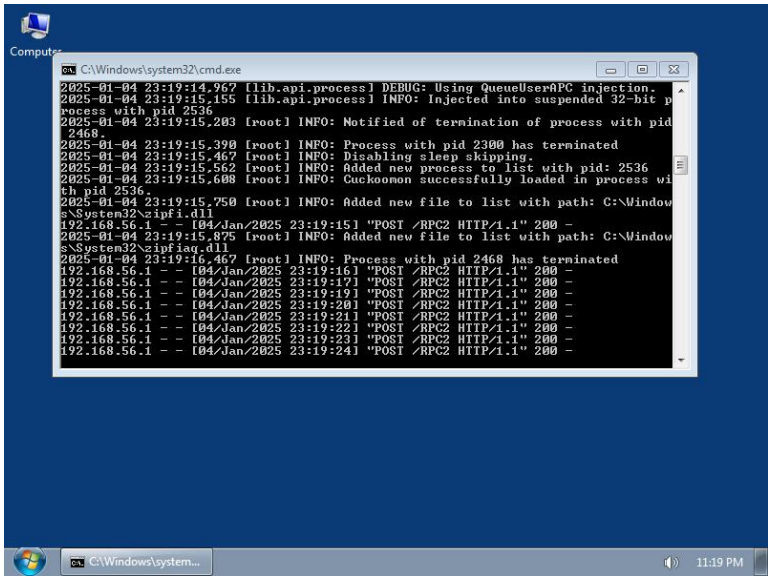

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:19:14,875 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [04/Jan/2025 23:19:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:14,921 [root] INFO: Added new process to list with pid: 2468
2025-01-04 23:19:14,921 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2468.
2025-01-04 23:19:14,967 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2536
2025-01-04 23:19:14,967 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:15,155 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2536
2025-01-04 23:19:15,203 [root] INFO: Notified of termination of process with pid
 2468.
2025-01-04 23:19:15,390 [root] INFO: Process with pid 2300 has terminated
2025-01-04 23:19:15,467 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:15,562 [root] INFO: Added new process to list with pid: 2536
2025-01-04 23:19:15,608 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2536.
2025-01-04 23:19:15,750 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfi.dll
192.168.56.1 - - [04/Jan/2025 23:19:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:15,875 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfiaq.dll
2025-01-04 23:19:16,467 [root] INFO: Process with pid 2468 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:16] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

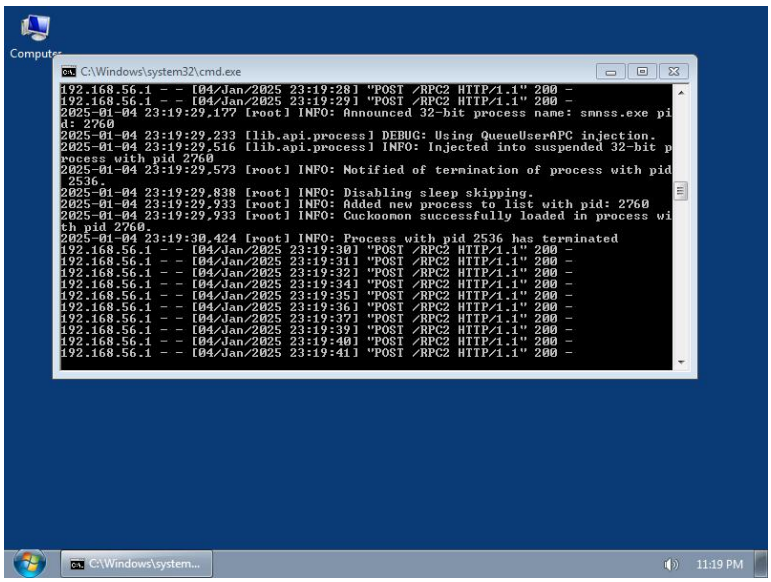

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,313 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2420
2025-01-04 23:21:21,313 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,815 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2420
192.168.56.1 - - [04/Jan/2025 23:21:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:22,427 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:22,486 [root] INFO: Added new process to list with pid: 2420
2025-01-04 23:21:22,486 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2420.
2025-01-04 23:21:22,711 [root] INFO: Notified of termination of process with pid
 2420.
2025-01-04 23:21:22,987 [root] INFO: Process with pid 2420 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

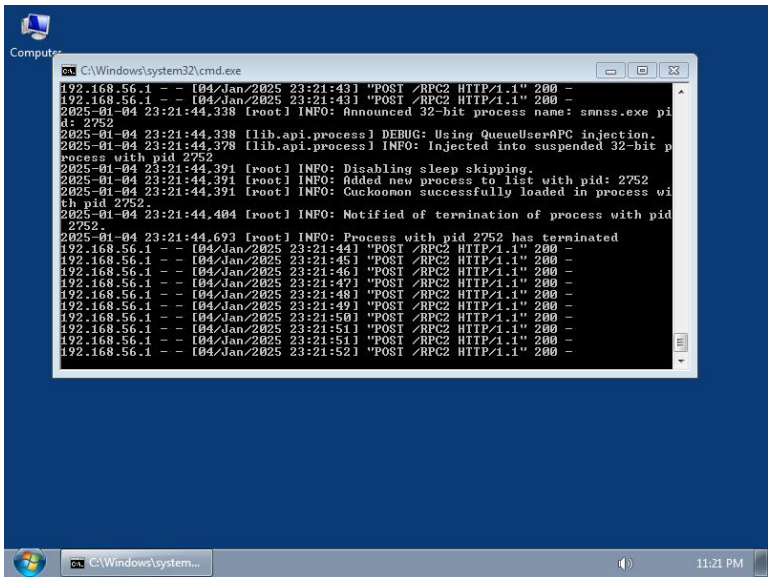

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:12] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:13,615 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2076
2025-01-04 23:20:13,615 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:13,799 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2076
192.168.56.1 - - [04/Jan/2025 23:20:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:14,130 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:14,171 [root] INFO: Added new process to list with pid: 2076
2025-01-04 23:20:14,171 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2076.
2025-01-04 23:20:14,171 [root] INFO: Notified of termination of process with pid
 2076.
2025-01-04 23:20:15,015 [root] INFO: Process with pid 2076 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:18] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

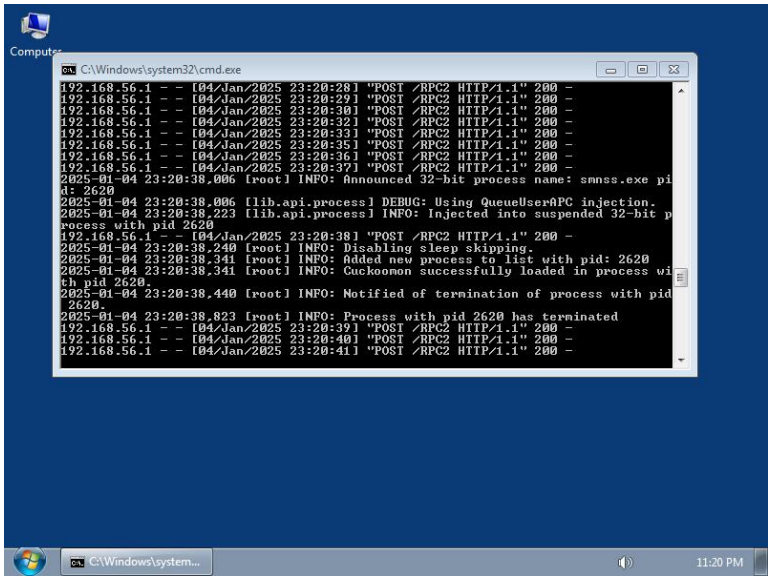

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:12] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:13,615 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2076
2025-01-04 23:20:13,615 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:13,799 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2076
192.168.56.1 - - [04/Jan/2025 23:20:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:14,130 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:14,171 [root] INFO: Added new process to list with pid: 2076
2025-01-04 23:20:14,171 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2076.
2025-01-04 23:20:14,171 [root] INFO: Notified of termination of process with pid
 2076.
2025-01-04 23:20:15,015 [root] INFO: Process with pid 2076 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:24] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

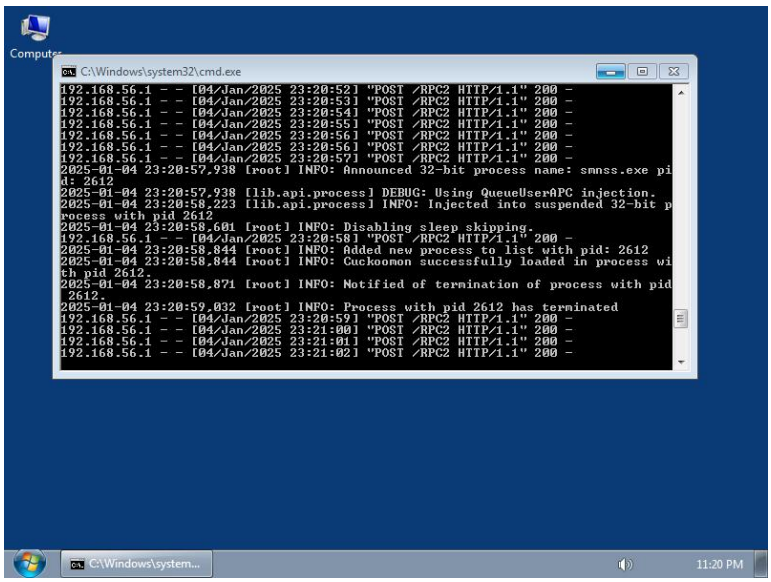

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:12] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:13,615 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2076
2025-01-04 23:20:13,615 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:13,799 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2076
192.168.56.1 - - [04/Jan/2025 23:20:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:14,130 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:14,171 [root] INFO: Added new process to list with pid: 2076
2025-01-04 23:20:14,171 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2076.
2025-01-04 23:20:14,171 [root] INFO: Notified of termination of process with pid
 2076.
2025-01-04 23:20:15,015 [root] INFO: Process with pid 2076 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:22] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

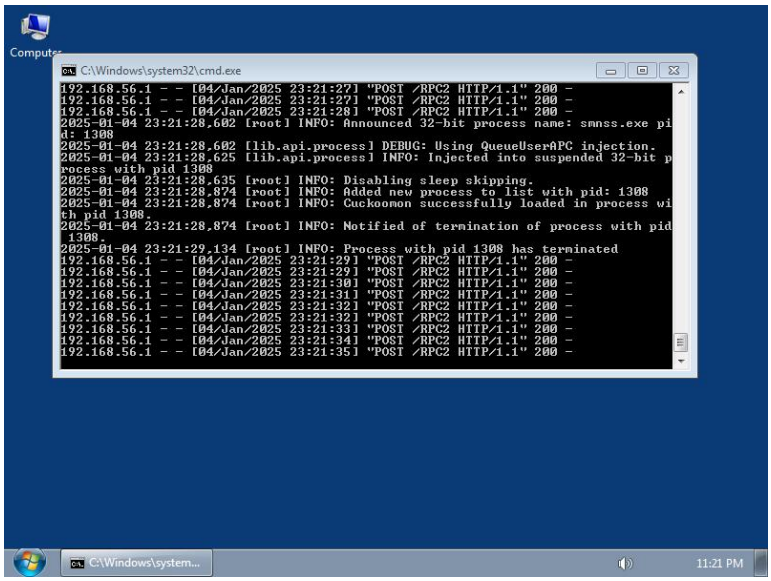

C:\Windows\system32\cmd.exe
2025-01-04 23:19:14,967 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:15,155 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2536
2025-01-04 23:19:15,203 [root] INFO: Notified of termination of process with pid
 2468.
2025-01-04 23:19:15,390 [root] INFO: Process with pid 2300 has terminated
2025-01-04 23:19:15,467 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:15,562 [root] INFO: Added new process to list with pid: 2536
2025-01-04 23:19:15,608 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2536.
2025-01-04 23:19:15,750 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfi.dll
192.168.56.1 - - [04/Jan/2025 23:19:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:15,875 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfiaq.dll
2025-01-04 23:19:16,467 [root] INFO: Process with pid 2468 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:24] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

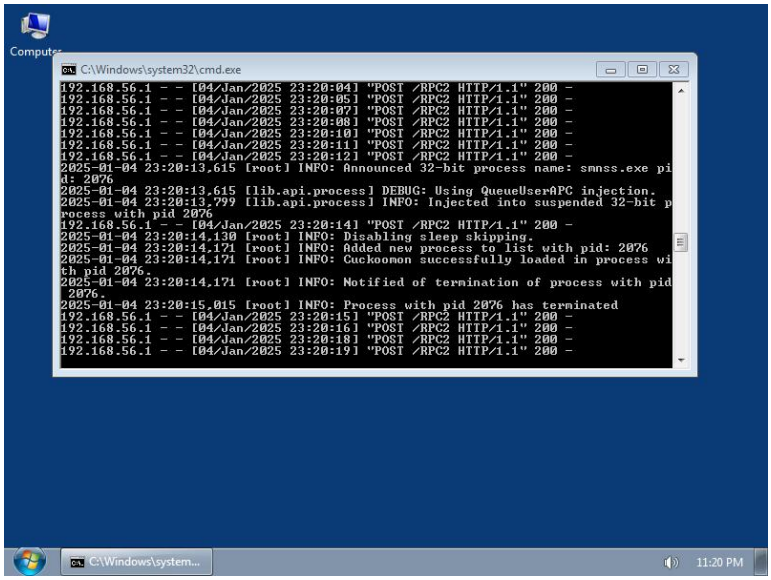

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:29] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:29,177 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2760
2025-01-04 23:19:29,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:29,516 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2760
2025-01-04 23:19:29,573 [root] INFO: Notified of termination of process with pid
 2536.
2025-01-04 23:19:29,838 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:29,933 [root] INFO: Added new process to list with pid: 2760
2025-01-04 23:19:29,933 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2760.
2025-01-04 23:19:30,424 [root] INFO: Process with pid 2536 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:41] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

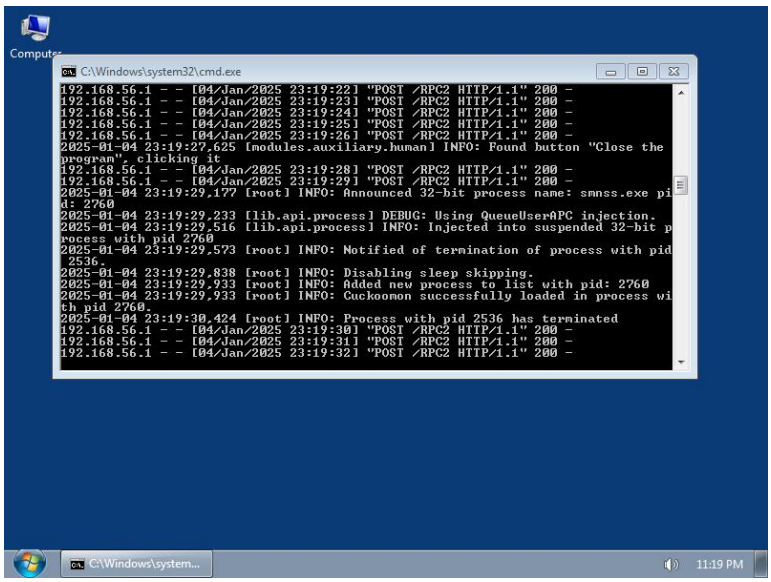

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:44,338 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2752
2025-01-04 23:21:44,338 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:44,378 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2752
2025-01-04 23:21:44,391 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:44,391 [root] INFO: Added new process to list with pid: 2752
2025-01-04 23:21:44,391 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2752.
2025-01-04 23:21:44,404 [root] INFO: Notified of termination of process with pid
2752.
2025-01-04 23:21:44,693 [root] INFO: Process with pid 2752 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:52] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

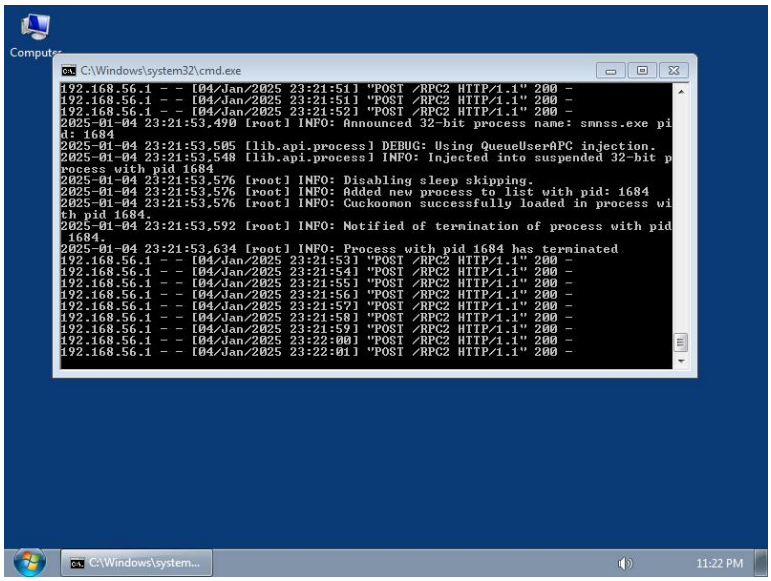

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:37] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,006 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2620
2025-01-04 23:20:38,006 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:38,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2620
192.168.56.1 - - [04/Jan/2025 23:20:38] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,240 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:38,341 [root] INFO: Added new process to list with pid: 2620
2025-01-04 23:20:38,341 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2620.
2025-01-04 23:20:38,440 [root] INFO: Notified of termination of process with pid
2620.
2025-01-04 23:20:38,823 [root] INFO: Process with pid 2620 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:41] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

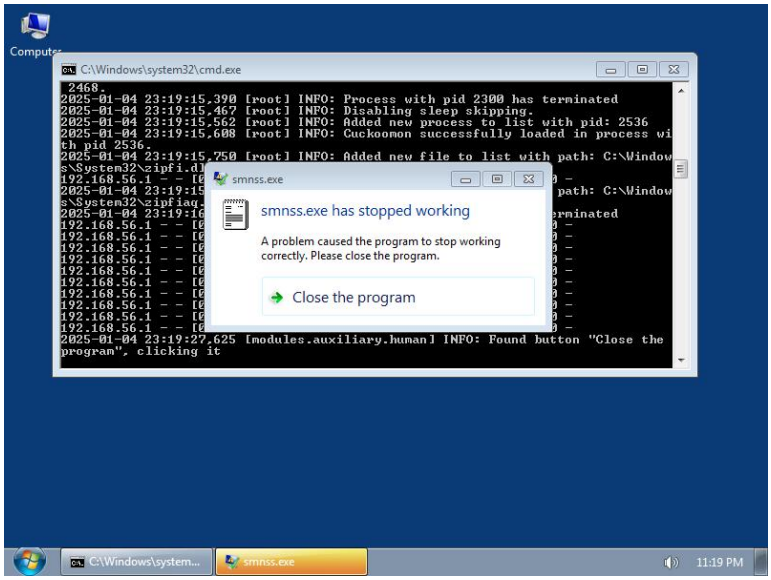

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:57] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:57,938 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2612
2025-01-04 23:20:57,938 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:58,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2612
2025-01-04 23:20:58,601 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [04/Jan/2025 23:20:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:58,844 [root] INFO: Added new process to list with pid: 2612
2025-01-04 23:20:58,844 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2612.
2025-01-04 23:20:58,871 [root] INFO: Notified of termination of process with pid
2612.
2025-01-04 23:20:59,032 [root] INFO: Process with pid 2612 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:02] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

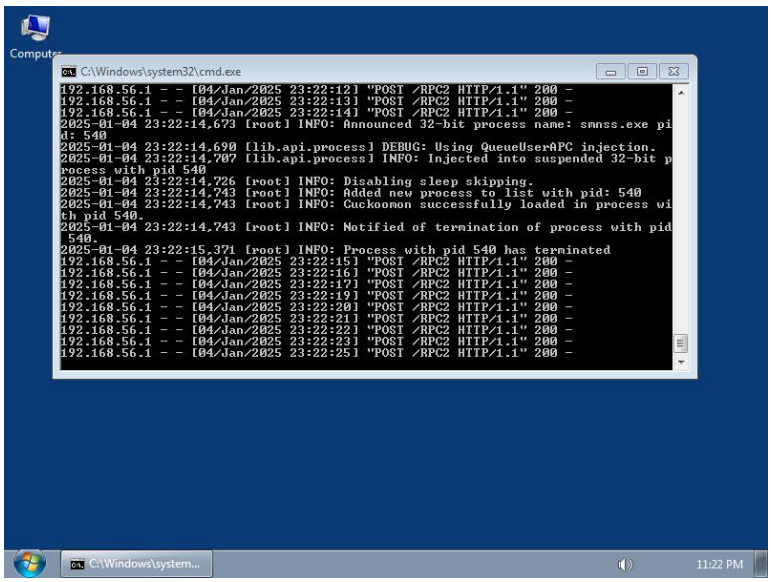

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:28] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:28,602 [root] INFO: Announced 32-bit process name: smnss.exe pid: 1308
2025-01-04 23:21:28,602 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:28,625 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 1308
2025-01-04 23:21:28,635 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:28,874 [root] INFO: Added new process to list with pid: 1308
2025-01-04 23:21:28,874 [root] INFO: Cuckoomon successfully loaded in process with pid 1308.
2025-01-04 23:21:28,874 [root] INFO: Notified of termination of process with pid 1308.
2025-01-04 23:21:29,134 [root] INFO: Process with pid 1308 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

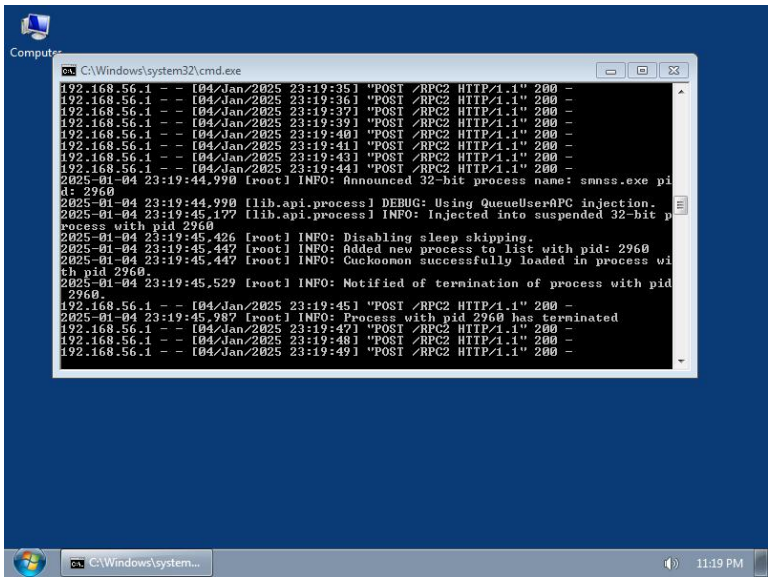

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:12] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:13,615 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2076
2025-01-04 23:20:13,615 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:13,799 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2076
192.168.56.1 - - [04/Jan/2025 23:20:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:14,130 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:14,171 [root] INFO: Added new process to list with pid: 2076
2025-01-04 23:20:14,171 [root] INFO: Cuckoomon successfully loaded in process with pid 2076.
2025-01-04 23:20:14,171 [root] INFO: Notified of termination of process with pid 2076.
2025-01-04 23:20:15,015 [root] INFO: Process with pid 2076 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:19] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

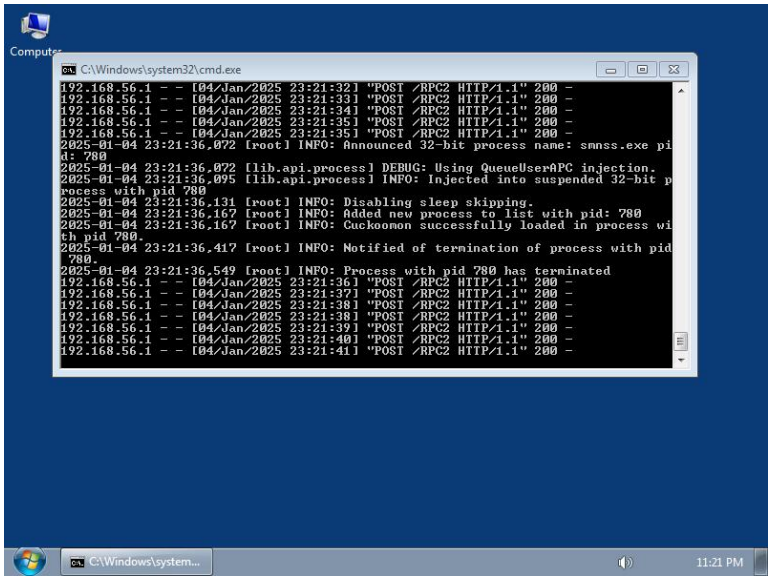

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:27,625 [modules.auxiliary.human] INFO: Found button "Close the program", clicking it
192.168.56.1 - - [04/Jan/2025 23:19:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:29] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:29,177 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2760
2025-01-04 23:19:29,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:29,516 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2760
2025-01-04 23:19:29,573 [root] INFO: Notified of termination of process with pid 2536.
2025-01-04 23:19:29,838 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:29,933 [root] INFO: Added new process to list with pid: 2760
2025-01-04 23:19:29,933 [root] INFO: Cuckoomon successfully loaded in process with pid 2760.
2025-01-04 23:19:30,424 [root] INFO: Process with pid 2536 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:32] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

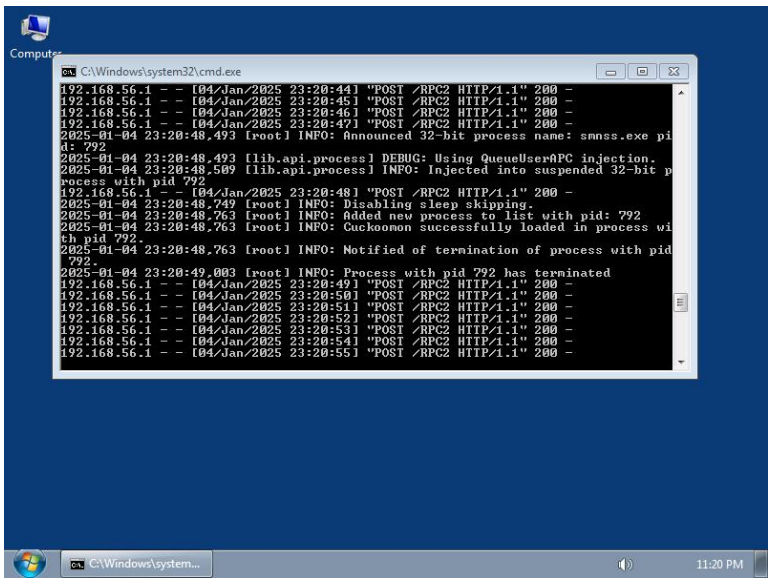

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:52] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:53,490 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1684
2025-01-04 23:21:53,505 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:53,548 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1684
2025-01-04 23:21:53,576 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:53,576 [root] INFO: Added new process to list with pid: 1684
2025-01-04 23:21:53,576 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1684.
2025-01-04 23:21:53,592 [root] INFO: Notified of termination of process with pid
1684.
2025-01-04 23:21:53,634 [root] INFO: Process with pid 1684 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:01] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

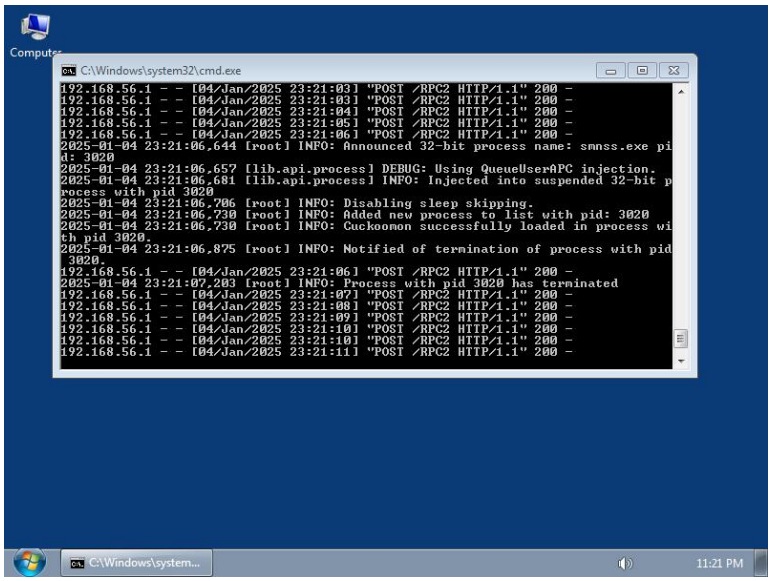

Computer
C:\Windows\system32\cmd.exe
2468.
2025-01-04 23:19:15,390 [root] INFO: Process with pid 2300 has terminated
2025-01-04 23:19:15,467 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:15,562 [root] INFO: Added new process to list with pid: 2536
2025-01-04 23:19:15,608 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2536.
2025-01-04 23:19:15,750 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfi.d
smnss.exe
smnss.exe has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
2025-01-04 23:19:27,625 [modules.auxiliary.human] INFO: Found button "Close the
program", clicking it
C:\Windows\system...
smnss.exe
11:19 PM

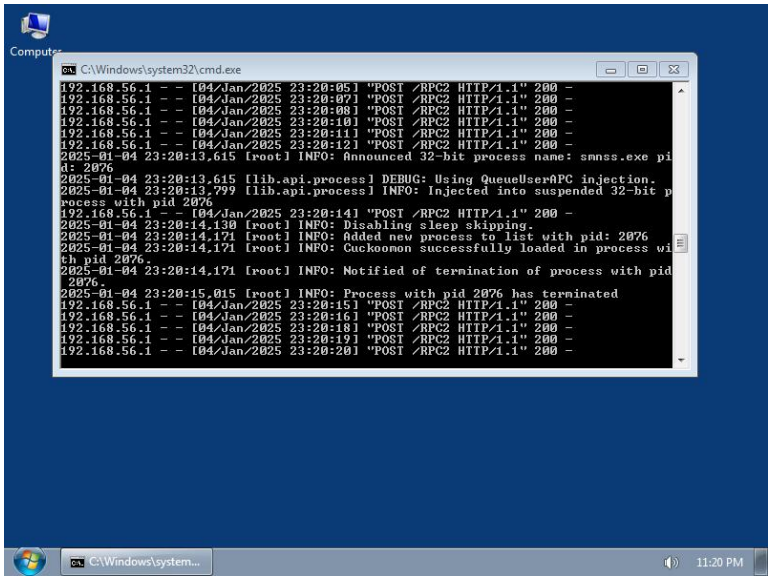

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:14,673 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 540
2025-01-04 23:22:14,690 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:14,707 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 540
2025-01-04 23:22:14,726 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:14,743 [root] INFO: Added new process to list with pid: 540
2025-01-04 23:22:14,743 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 540.
2025-01-04 23:22:14,743 [root] INFO: Notified of termination of process with pid
540.
2025-01-04 23:22:15,371 [root] INFO: Process with pid 540 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:25] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

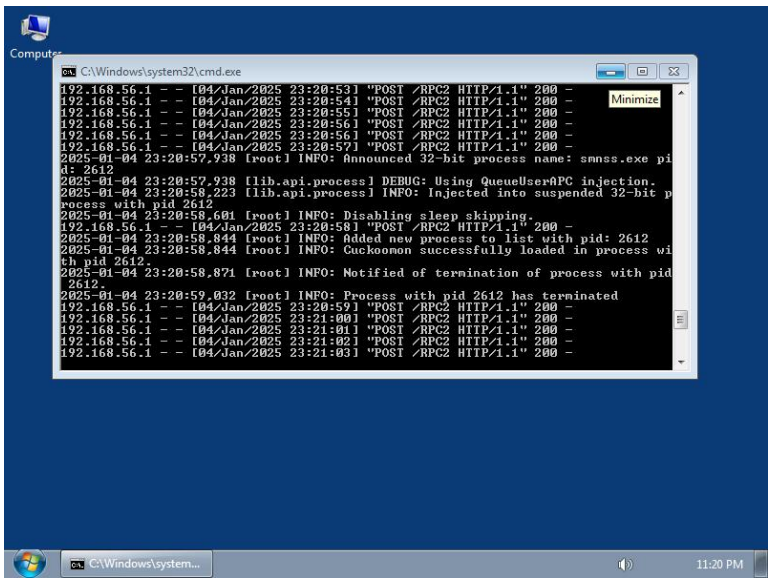

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:44] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:44,990 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2960
2025-01-04 23:19:44,990 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:45,177 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2960
2025-01-04 23:19:45,426 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:45,447 [root] INFO: Added new process to list with pid: 2960
2025-01-04 23:19:45,447 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2960.
2025-01-04 23:19:45,529 [root] INFO: Notified of termination of process with pid
 2960.
192.168.56.1 - - [04/Jan/2025 23:19:45] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:45,987 [root] INFO: Process with pid 2960 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:49] "POST /RPC2 HTTP/1.1" 200 -
11:19 PM

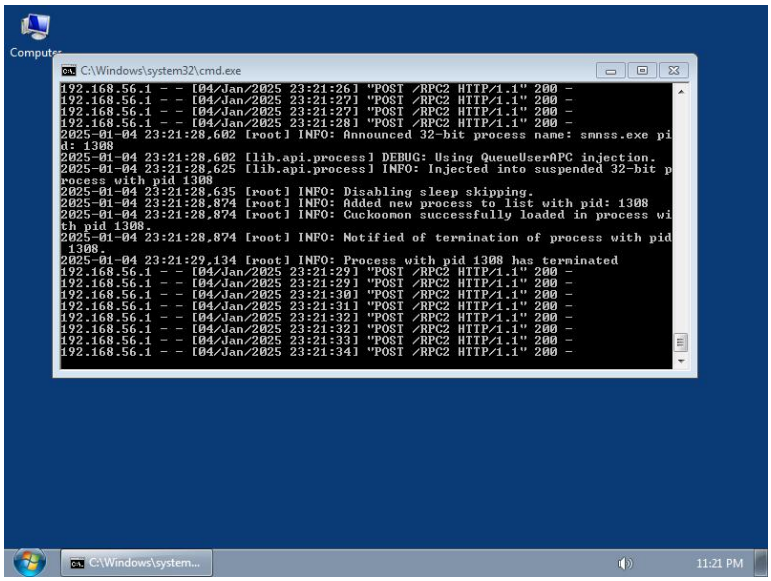

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:36,072 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 780
2025-01-04 23:21:36,072 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:36,095 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 780
2025-01-04 23:21:36,131 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:36,167 [root] INFO: Added new process to list with pid: 780
2025-01-04 23:21:36,167 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 780.
2025-01-04 23:21:36,417 [root] INFO: Notified of termination of process with pid
 780.
2025-01-04 23:21:36,549 [root] INFO: Process with pid 780 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:41] "POST /RPC2 HTTP/1.1" 200 -
11:21 PM

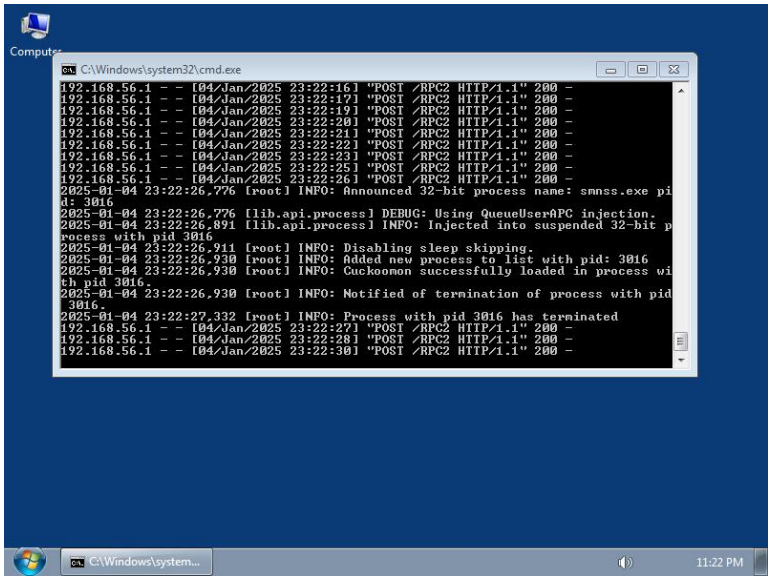

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:47] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,493 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 792
2025-01-04 23:20:48,493 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:48,509 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 792
192.168.56.1 - - [04/Jan/2025 23:20:48] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,749 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:48,763 [root] INFO: Added new process to list with pid: 792
2025-01-04 23:20:48,763 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 792.
2025-01-04 23:20:48,763 [root] INFO: Notified of termination of process with pid
 792.
2025-01-04 23:20:49,003 [root] INFO: Process with pid 792 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:55] "POST /RPC2 HTTP/1.1" 200 -
11:20 PM

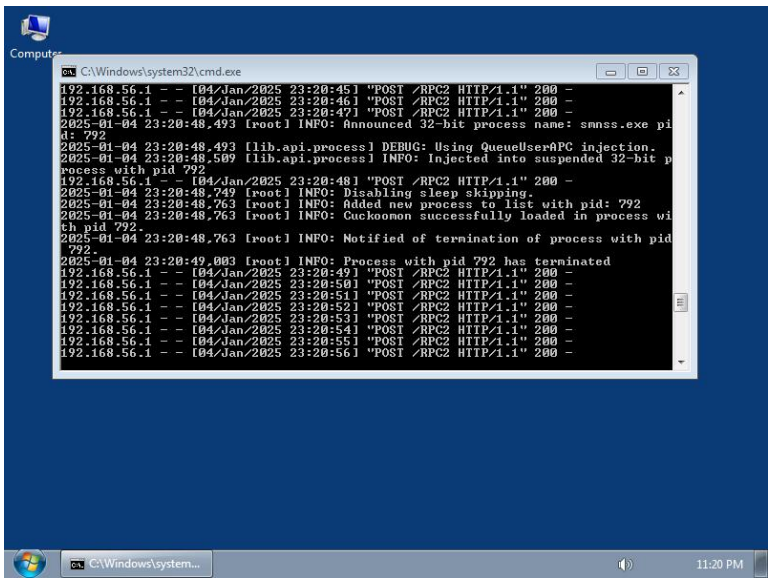

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:06,644 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3020
2025-01-04 23:21:06,657 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:06,681 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3020
2025-01-04 23:21:06,706 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:06,730 [root] INFO: Added new process to list with pid: 3020
2025-01-04 23:21:06,730 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3020.
2025-01-04 23:21:06,875 [root] INFO: Notified of termination of process with pid
 3020.
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:07,203 [root] INFO: Process with pid 3020 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:11] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

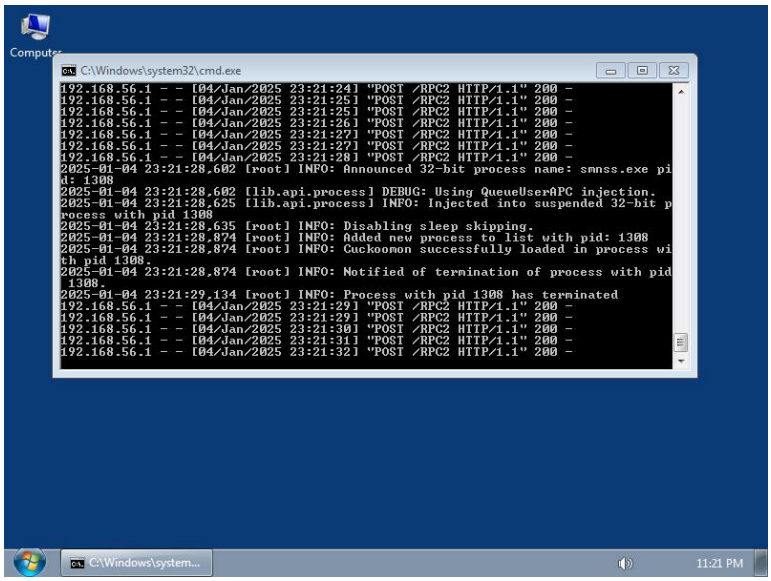

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:12] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:13,615 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2076
2025-01-04 23:20:13,615 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:13,799 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2076
192.168.56.1 - - [04/Jan/2025 23:20:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:14,130 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:14,171 [root] INFO: Added new process to list with pid: 2076
2025-01-04 23:20:14,171 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2076.
2025-01-04 23:20:14,171 [root] INFO: Notified of termination of process with pid
 2076.
2025-01-04 23:20:15,015 [root] INFO: Process with pid 2076 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:20] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

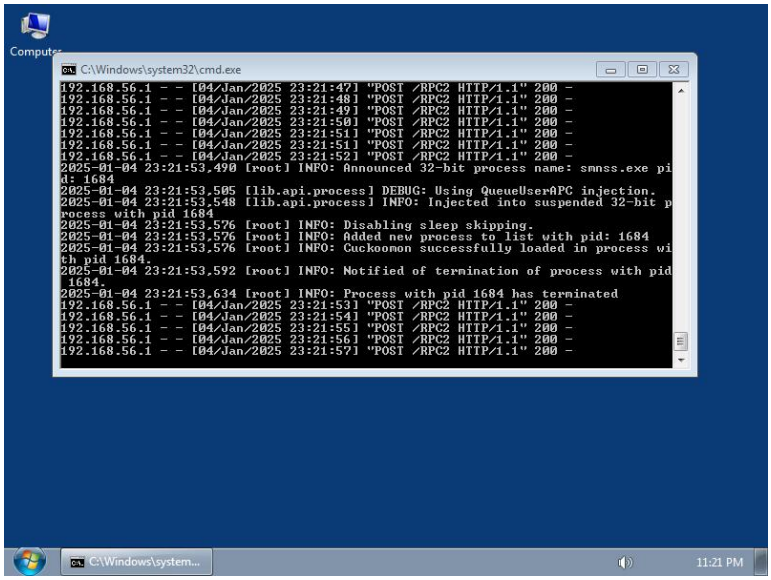

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:57] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:57,938 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2612
2025-01-04 23:20:57,938 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:58,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2612
2025-01-04 23:20:58,601 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [04/Jan/2025 23:20:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:58,844 [root] INFO: Added new process to list with pid: 2612
2025-01-04 23:20:58,844 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2612.
2025-01-04 23:20:58,871 [root] INFO: Notified of termination of process with pid
 2612.
2025-01-04 23:20:59,032 [root] INFO: Process with pid 2612 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
Minimize
C:\Windows\system...
11:20 PM

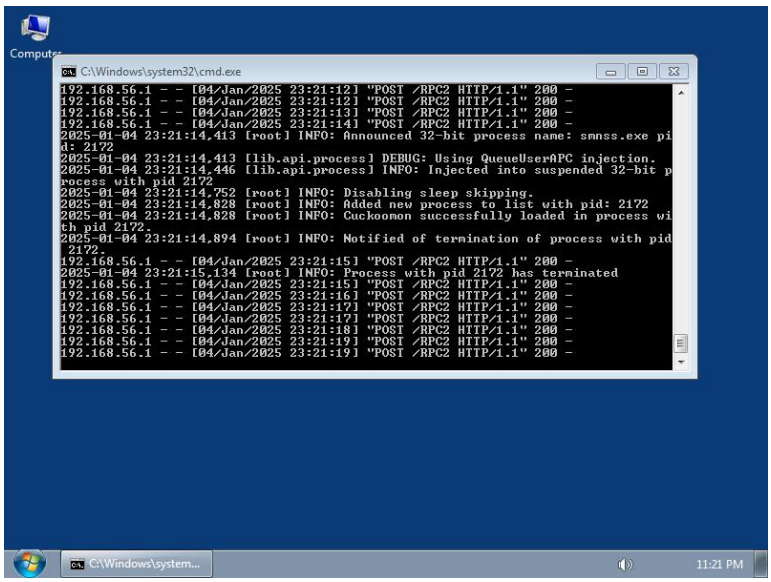

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:28] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:28,602 [root] INFO: Announced 32-bit process name: smnss.exe pid: 1308
2025-01-04 23:21:28,602 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:28,625 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 1308
2025-01-04 23:21:28,635 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:28,874 [root] INFO: Added new process to list with pid: 1308
2025-01-04 23:21:28,874 [root] INFO: Cuckoomon successfully loaded in process with pid 1308.
2025-01-04 23:21:28,874 [root] INFO: Notified of termination of process with pid 1308.
2025-01-04 23:21:29,134 [root] INFO: Process with pid 1308 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:34] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

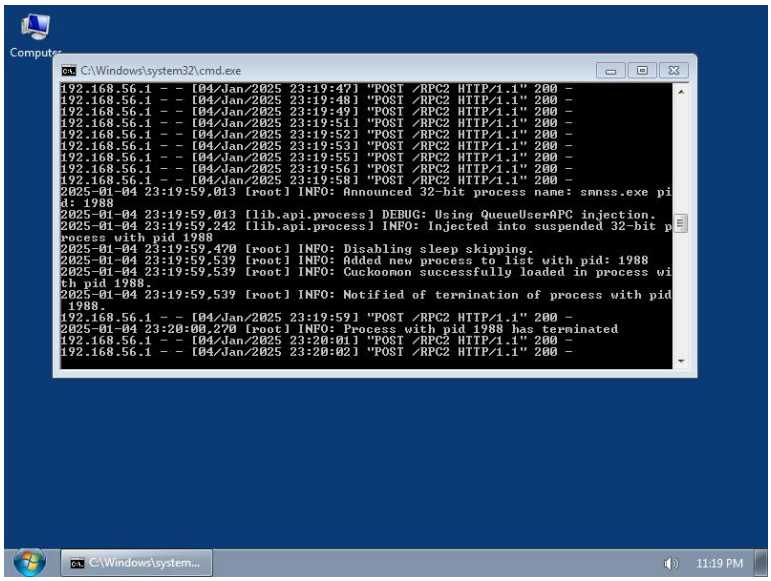

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:26,776 [root] INFO: Announced 32-bit process name: smnss.exe pid: 3016
2025-01-04 23:22:26,776 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:26,891 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 3016
2025-01-04 23:22:26,911 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:26,930 [root] INFO: Added new process to list with pid: 3016
2025-01-04 23:22:26,930 [root] INFO: Cuckoomon successfully loaded in process with pid 3016.
2025-01-04 23:22:26,930 [root] INFO: Notified of termination of process with pid 3016.
2025-01-04 23:22:27,332 [root] INFO: Process with pid 3016 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:30] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

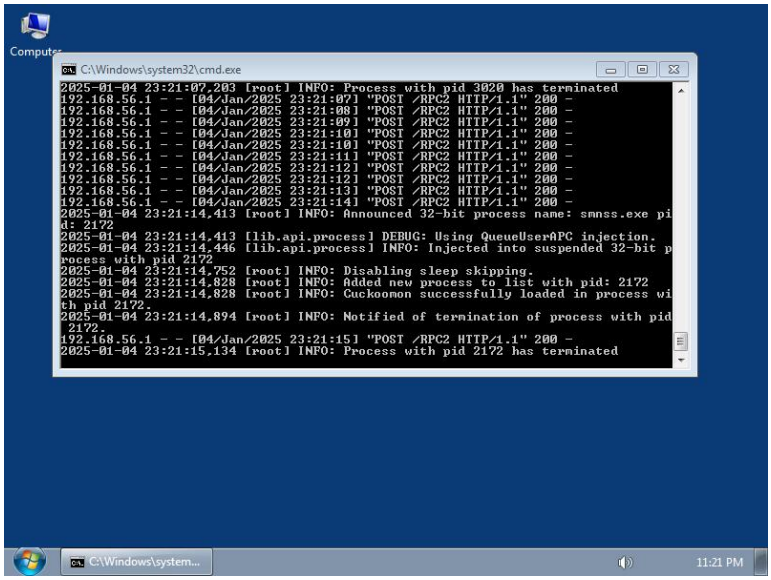

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:47] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,493 [root] INFO: Announced 32-bit process name: smnss.exe pid: 792
2025-01-04 23:20:48,493 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:48,509 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 792
192.168.56.1 - - [04/Jan/2025 23:20:48] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,749 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:48,763 [root] INFO: Added new process to list with pid: 792
2025-01-04 23:20:48,763 [root] INFO: Cuckoomon successfully loaded in process with pid 792.
2025-01-04 23:20:48,763 [root] INFO: Notified of termination of process with pid 792.
2025-01-04 23:20:49,003 [root] INFO: Process with pid 792 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

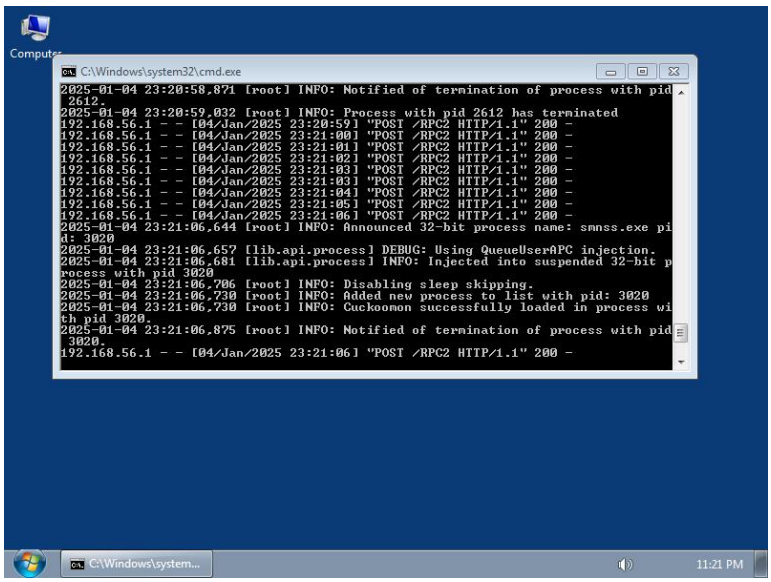

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:28] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:28,602 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1308
2025-01-04 23:21:28,602 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:28,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1308
2025-01-04 23:21:28,635 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:28,874 [root] INFO: Added new process to list with pid: 1308
2025-01-04 23:21:28,874 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1308.
2025-01-04 23:21:28,874 [root] INFO: Notified of termination of process with pid
 1308.
2025-01-04 23:21:29,134 [root] INFO: Process with pid 1308 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

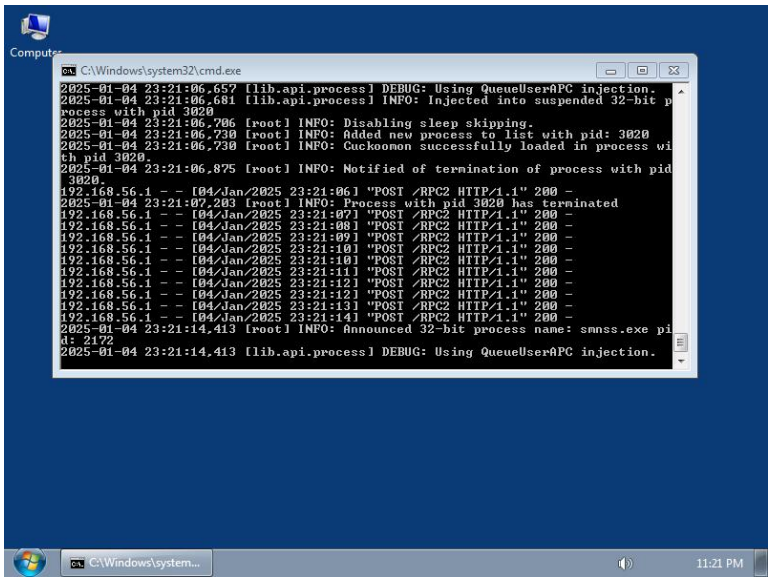

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:52] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:53,490 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1684
2025-01-04 23:21:53,505 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:53,548 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1684
2025-01-04 23:21:53,576 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:53,576 [root] INFO: Added new process to list with pid: 1684
2025-01-04 23:21:53,576 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1684.
2025-01-04 23:21:53,592 [root] INFO: Notified of termination of process with pid
 1684.
2025-01-04 23:21:53,634 [root] INFO: Process with pid 1684 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:57] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

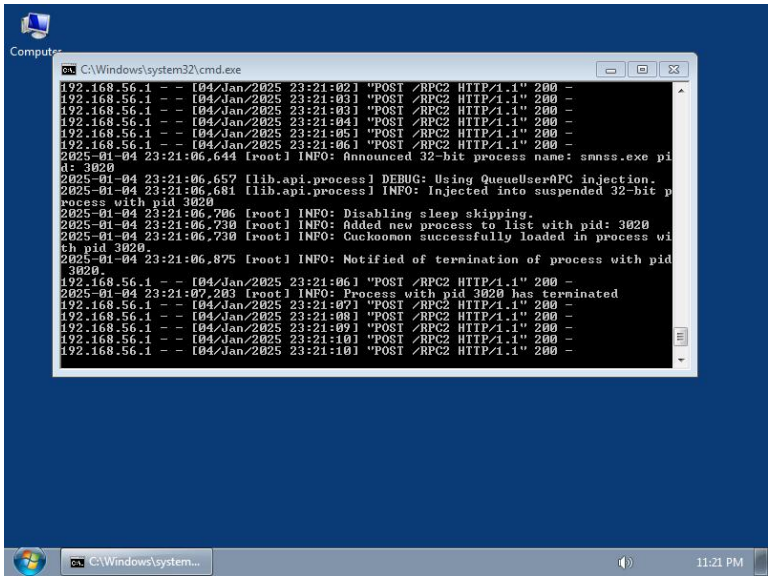

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:14,413 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2172
2025-01-04 23:21:14,413 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:14,446 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2172
2025-01-04 23:21:14,752 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:14,828 [root] INFO: Added new process to list with pid: 2172
2025-01-04 23:21:14,828 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2172.
2025-01-04 23:21:14,894 [root] INFO: Notified of termination of process with pid
 2172.
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:15,134 [root] INFO: Process with pid 2172 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

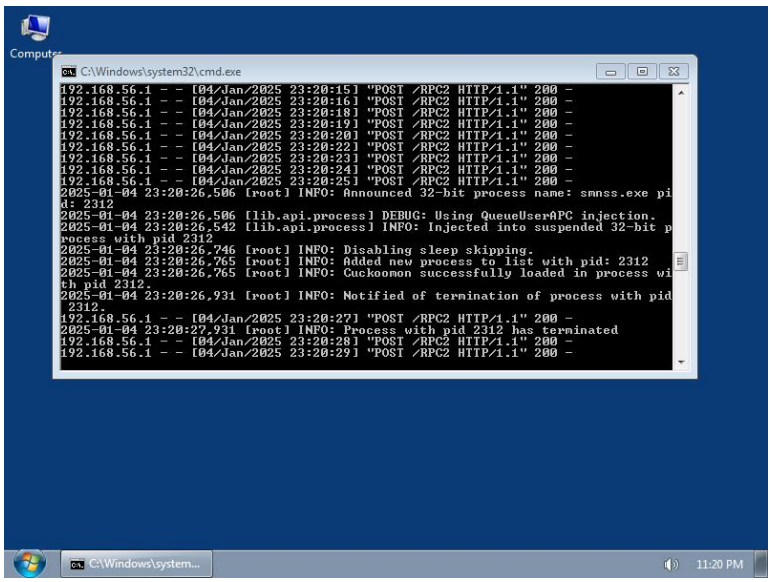

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:59,013 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1988
2025-01-04 23:19:59,013 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:59,242 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1988
2025-01-04 23:19:59,470 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:59,539 [root] INFO: Added new process to list with pid: 1988
2025-01-04 23:19:59,539 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1988.
2025-01-04 23:19:59,539 [root] INFO: Notified of termination of process with pid
 1988.
192.168.56.1 - - [04/Jan/2025 23:19:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:00,270 [root] INFO: Process with pid 1988 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:02] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

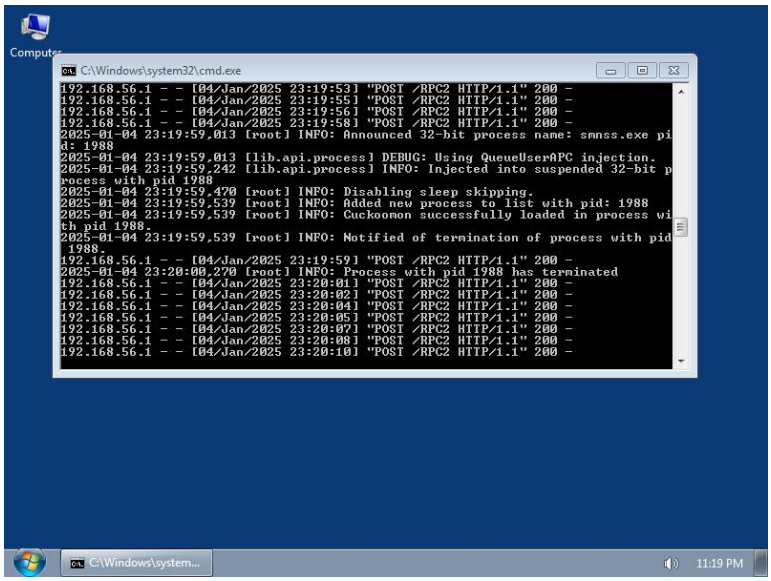

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:21:07,203 [root] INFO: Process with pid 3020 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:14,413 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2172
2025-01-04 23:21:14,413 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:14,446 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2172
2025-01-04 23:21:14,752 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:14,828 [root] INFO: Added new process to list with pid: 2172
2025-01-04 23:21:14,828 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2172.
2025-01-04 23:21:14,894 [root] INFO: Notified of termination of process with pid
 2172.
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:15,134 [root] INFO: Process with pid 2172 has terminated
C:\Windows\system...
11:21 PM

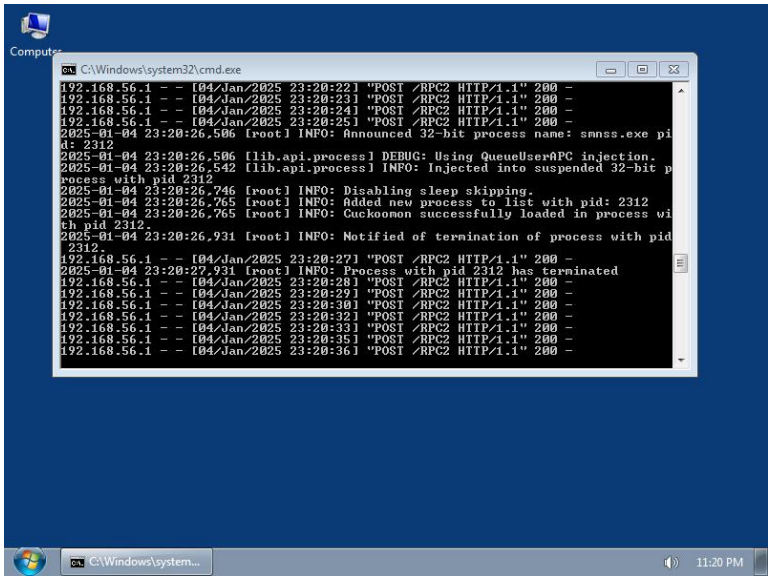

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:20:58,871 [root] INFO: Notified of termination of process with pid
 2612.
2025-01-04 23:20:59,032 [root] INFO: Process with pid 2612 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:06,644 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3020
2025-01-04 23:21:06,657 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:06,681 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3020
2025-01-04 23:21:06,706 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:06,730 [root] INFO: Added new process to list with pid: 3020
2025-01-04 23:21:06,730 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3020.
2025-01-04 23:21:06,875 [root] INFO: Notified of termination of process with pid
 3020.
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

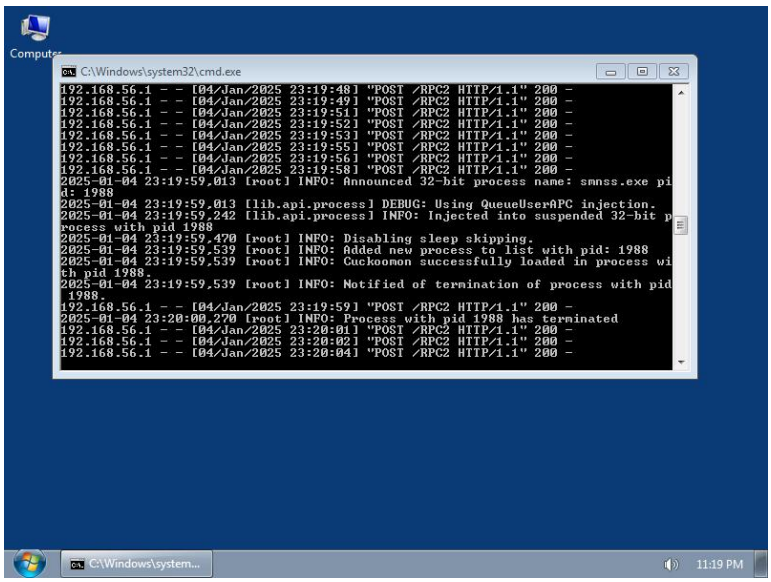

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:21:06,657 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:06,681 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 3020
2025-01-04 23:21:06,706 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:06,730 [root] INFO: Added new process to list with pid: 3020
2025-01-04 23:21:06,730 [root] INFO: Cuckoomon successfully loaded in process with pid 3020.
2025-01-04 23:21:06,875 [root] INFO: Notified of termination of process with pid 3020.
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:07,203 [root] INFO: Process with pid 3020 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:14,413 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2172
2025-01-04 23:21:14,413 [lib.api.process] DEBUG: Using QueueUserAPC injection.
C:\Windows\system...
11:21 PM

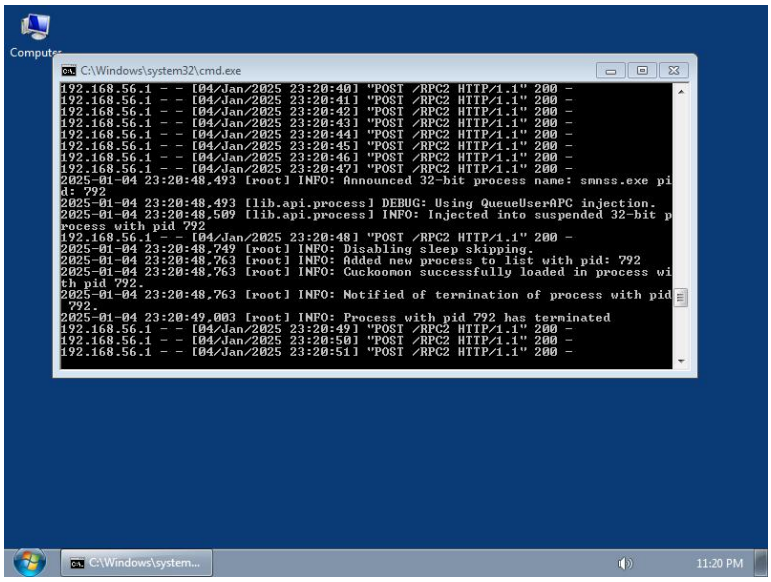

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:06,644 [root] INFO: Announced 32-bit process name: smnss.exe pid: 3020
2025-01-04 23:21:06,657 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:06,681 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 3020
2025-01-04 23:21:06,706 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:06,730 [root] INFO: Added new process to list with pid: 3020
2025-01-04 23:21:06,730 [root] INFO: Cuckoomon successfully loaded in process with pid 3020.
2025-01-04 23:21:06,875 [root] INFO: Notified of termination of process with pid 3020.
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:07,203 [root] INFO: Process with pid 3020 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

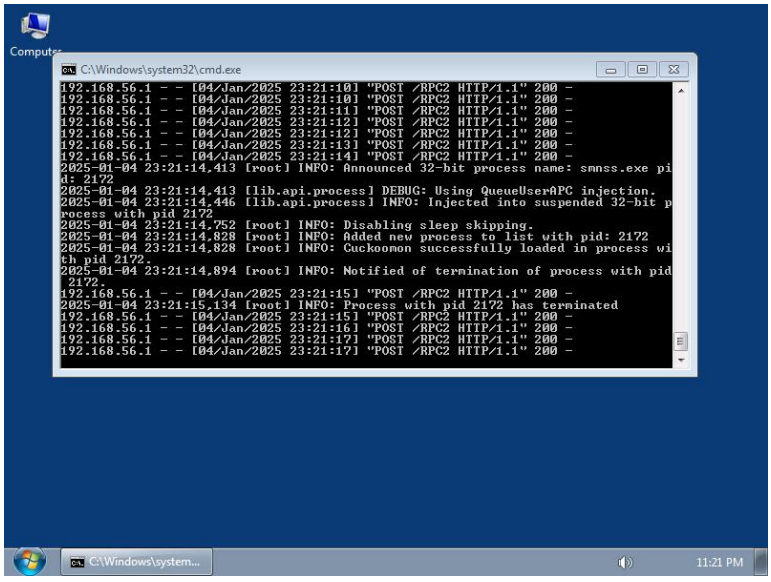

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:25] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:26,506 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2312
2025-01-04 23:20:26,506 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:26,542 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2312
2025-01-04 23:20:26,746 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:26,765 [root] INFO: Added new process to list with pid: 2312
2025-01-04 23:20:26,765 [root] INFO: Cuckoomon successfully loaded in process with pid 2312.
2025-01-04 23:20:26,931 [root] INFO: Notified of termination of process with pid 2312.
192.168.56.1 - - [04/Jan/2025 23:20:27] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:27,931 [root] INFO: Process with pid 2312 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:29] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

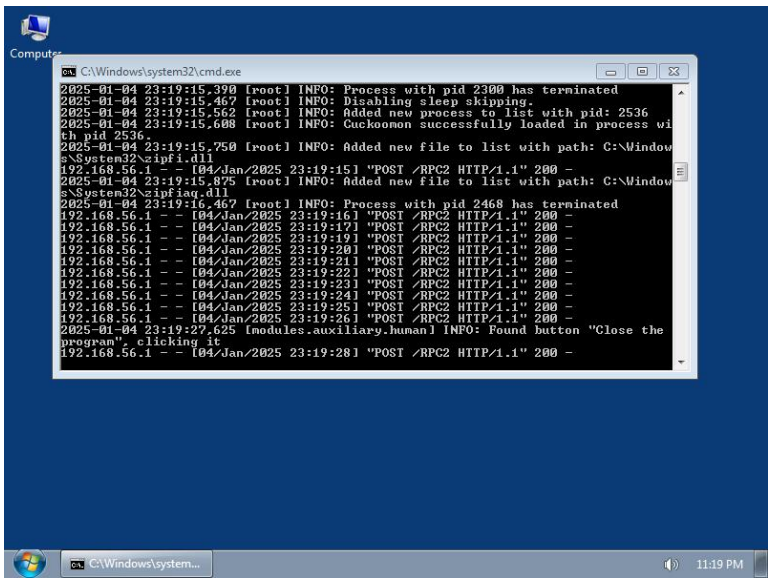

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:59,013 [root] INFO: Announced 32-bit process name: smnss.exe pid: 1988
2025-01-04 23:19:59,013 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:59,242 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 1988
2025-01-04 23:19:59,470 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:59,539 [root] INFO: Added new process to list with pid: 1988
2025-01-04 23:19:59,539 [root] INFO: Cuckoomon successfully loaded in process with pid 1988.
2025-01-04 23:19:59,539 [root] INFO: Notified of termination of process with pid 1988.
192.168.56.1 - - [04/Jan/2025 23:19:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:00,270 [root] INFO: Process with pid 1988 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:10] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

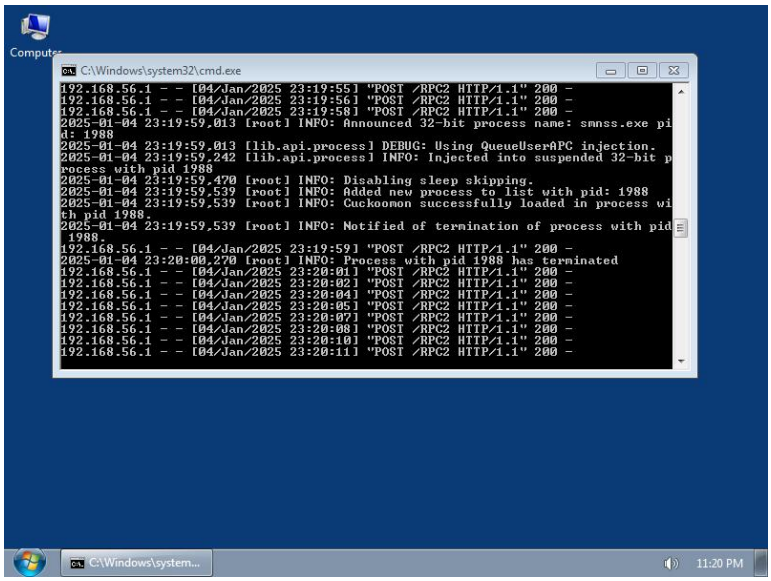

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:25] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:26,506 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2312
2025-01-04 23:20:26,506 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:26,542 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2312
2025-01-04 23:20:26,746 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:26,765 [root] INFO: Added new process to list with pid: 2312
2025-01-04 23:20:26,765 [root] INFO: Cuckoomon successfully loaded in process with pid 2312.
2025-01-04 23:20:26,931 [root] INFO: Notified of termination of process with pid 2312.
192.168.56.1 - - [04/Jan/2025 23:20:27] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:27,931 [root] INFO: Process with pid 2312 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:36] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

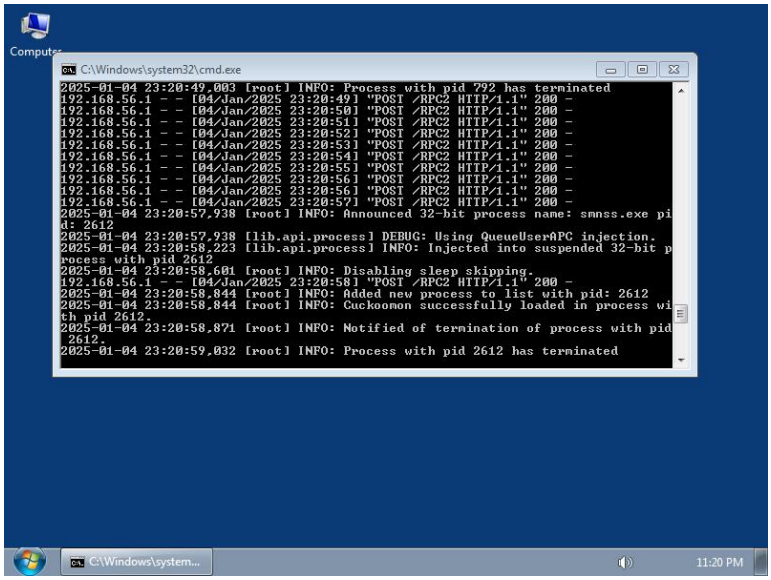

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:59,013 [root] INFO: Announced 32-bit process name: smnss.exe pid: 1988
2025-01-04 23:19:59,013 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:59,242 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 1988
2025-01-04 23:19:59,470 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:59,539 [root] INFO: Added new process to list with pid: 1988
2025-01-04 23:19:59,539 [root] INFO: Cuckoomon successfully loaded in process with pid 1988.
2025-01-04 23:19:59,539 [root] INFO: Notified of termination of process with pid 1988.
192.168.56.1 - - [04/Jan/2025 23:19:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:00,270 [root] INFO: Process with pid 1988 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:04] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

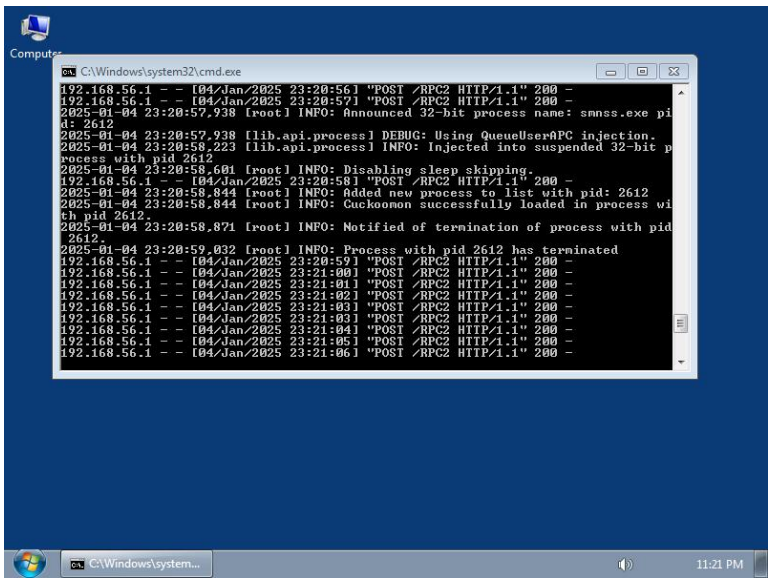

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:47] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,493 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 792
2025-01-04 23:20:48,493 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:48,509 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 792
192.168.56.1 - - [04/Jan/2025 23:20:48] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,749 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:48,763 [root] INFO: Added new process to list with pid: 792
2025-01-04 23:20:48,763 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 792.
2025-01-04 23:20:48,763 [root] INFO: Notified of termination of process with pid
 792.
2025-01-04 23:20:49,003 [root] INFO: Process with pid 792 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:51] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

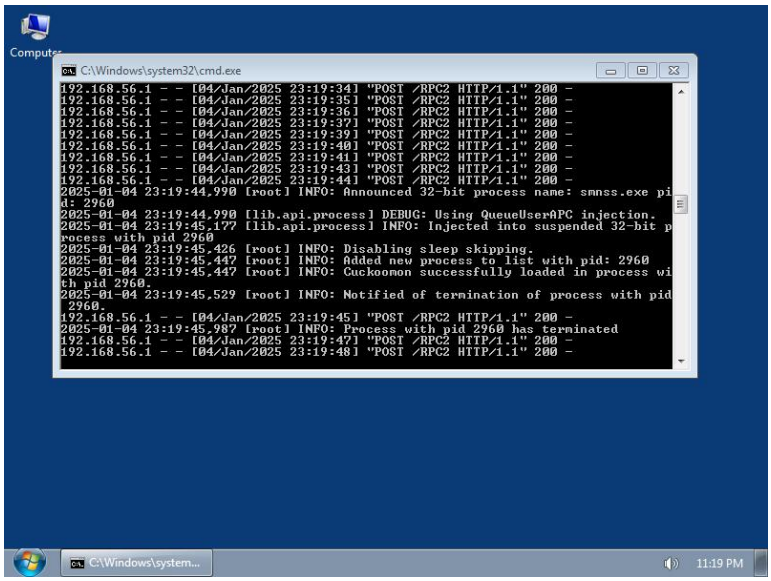

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:14,413 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2172
2025-01-04 23:21:14,413 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:14,446 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2172
2025-01-04 23:21:14,752 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:14,828 [root] INFO: Added new process to list with pid: 2172
2025-01-04 23:21:14,828 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2172.
2025-01-04 23:21:14,894 [root] INFO: Notified of termination of process with pid
 2172.
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:15,134 [root] INFO: Process with pid 2172 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

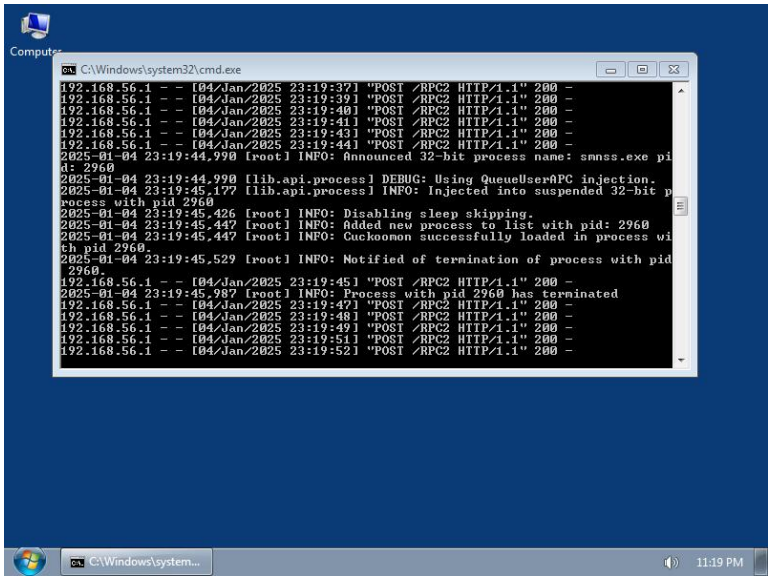

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:19:15,390 [root] INFO: Process with pid 2300 has terminated
2025-01-04 23:19:15,467 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:15,562 [root] INFO: Added new process to list with pid: 2536
2025-01-04 23:19:15,608 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2536.
2025-01-04 23:19:15,750 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfi.dll
192.168.56.1 - - [04/Jan/2025 23:19:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:15,875 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfiaq.dll
2025-01-04 23:19:16,467 [root] INFO: Process with pid 2468 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:27,625 [modules.auxiliary.human] INFO: Found button "Close the
program", clicking it
192.168.56.1 - - [04/Jan/2025 23:19:28] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

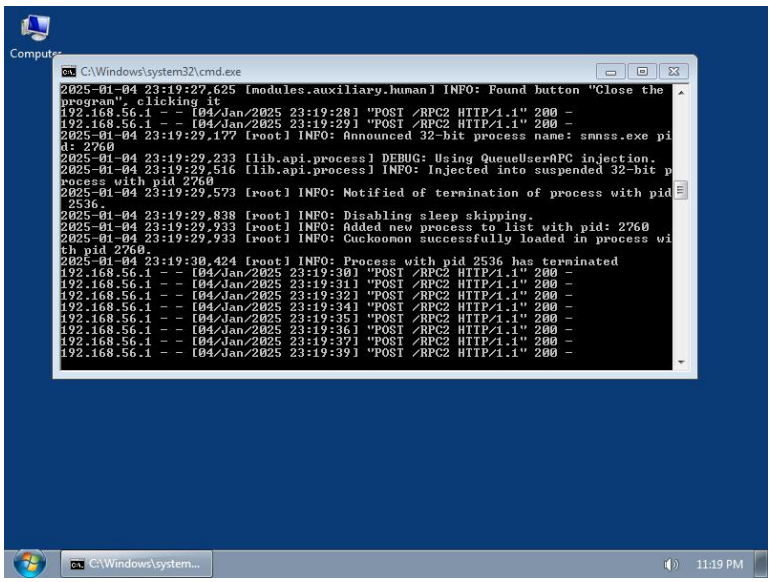

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:59,013 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1988
2025-01-04 23:19:59,013 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:59,242 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1988
2025-01-04 23:19:59,470 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:59,539 [root] INFO: Added new process to list with pid: 1988
2025-01-04 23:19:59,539 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1988.
2025-01-04 23:19:59,539 [root] INFO: Notified of termination of process with pid
 1988.
192.168.56.1 - - [04/Jan/2025 23:19:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:00,270 [root] INFO: Process with pid 1988 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:11] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

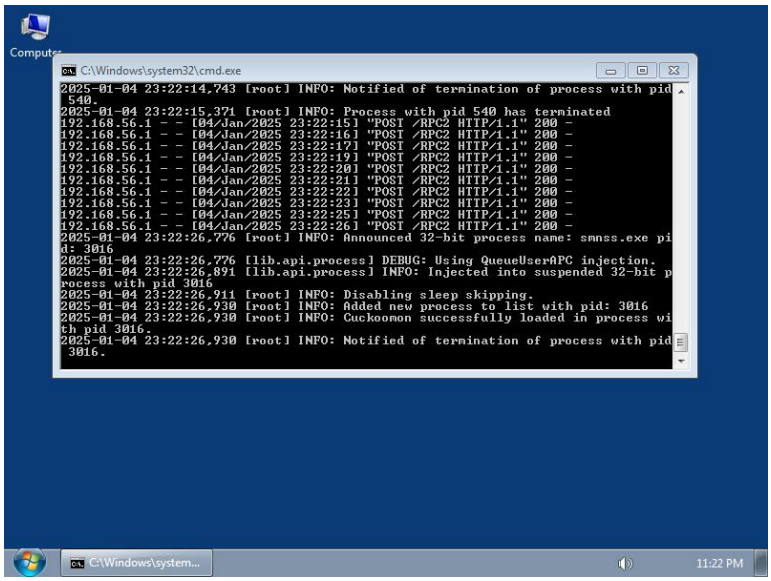

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:20:49,003 [root] INFO: Process with pid 792 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:57] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:57,938 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2612
2025-01-04 23:20:57,938 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:58,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2612
2025-01-04 23:20:58,601 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [04/Jan/2025 23:20:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:58,844 [root] INFO: Added new process to list with pid: 2612
2025-01-04 23:20:58,844 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2612.
2025-01-04 23:20:58,871 [root] INFO: Notified of termination of process with pid
 2612.
2025-01-04 23:20:59,032 [root] INFO: Process with pid 2612 has terminated
C:\Windows\system...
11:20 PM

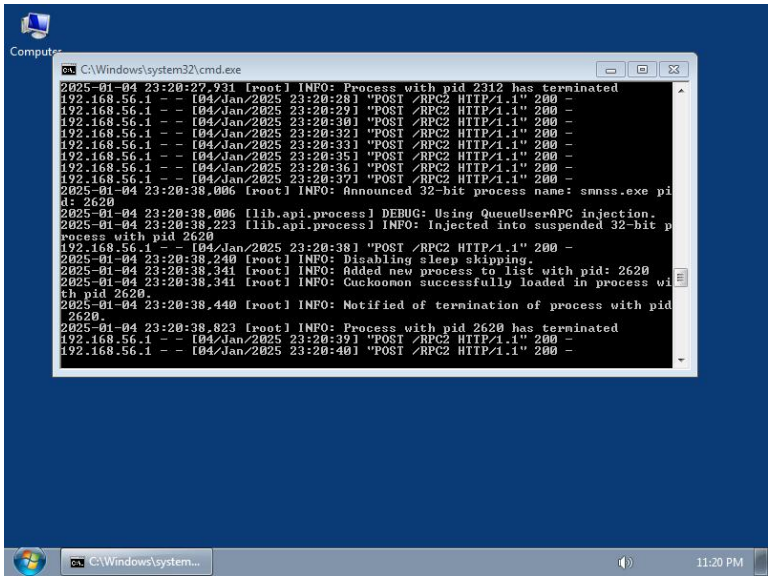

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:57] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:57,938 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2612
2025-01-04 23:20:57,938 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:58,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2612
2025-01-04 23:20:58,601 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [04/Jan/2025 23:20:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:58,844 [root] INFO: Added new process to list with pid: 2612
2025-01-04 23:20:58,844 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2612.
2025-01-04 23:20:58,871 [root] INFO: Notified of termination of process with pid
 2612.
2025-01-04 23:20:59,032 [root] INFO: Process with pid 2612 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

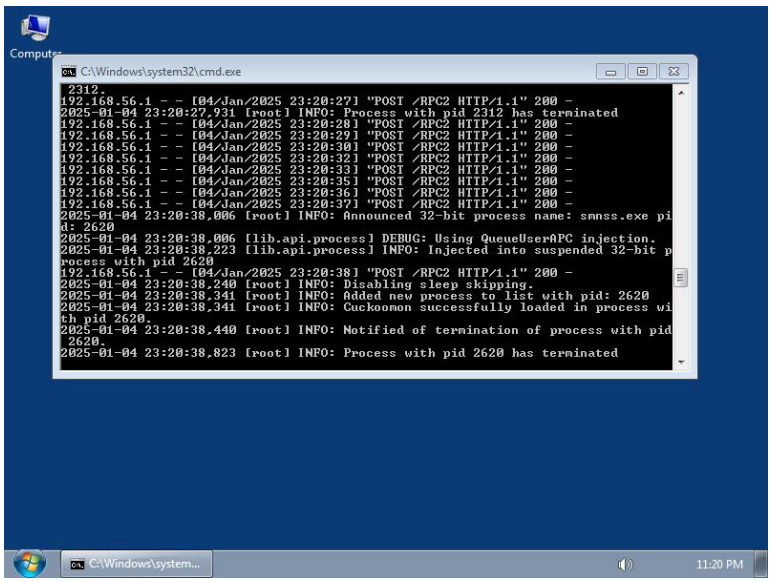

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:44] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:44,990 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2960
2025-01-04 23:19:44,990 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:45,177 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2960
2025-01-04 23:19:45,426 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:45,447 [root] INFO: Added new process to list with pid: 2960
2025-01-04 23:19:45,447 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2960.
2025-01-04 23:19:45,529 [root] INFO: Notified of termination of process with pid
 2960.
192.168.56.1 - - [04/Jan/2025 23:19:45] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:45,987 [root] INFO: Process with pid 2960 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:48] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

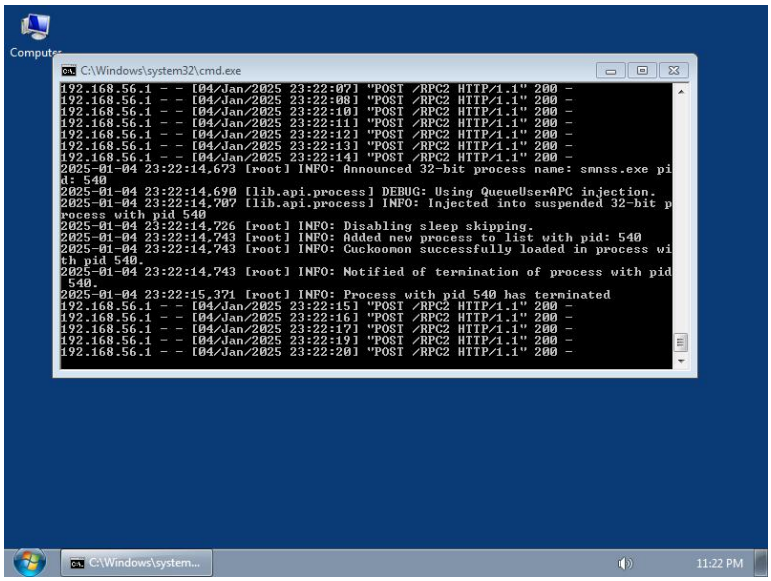

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:44] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:44,990 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2960
2025-01-04 23:19:44,990 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:45,177 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2960
2025-01-04 23:19:45,426 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:45,447 [root] INFO: Added new process to list with pid: 2960
2025-01-04 23:19:45,447 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2960.
2025-01-04 23:19:45,529 [root] INFO: Notified of termination of process with pid
 2960.
192.168.56.1 - - [04/Jan/2025 23:19:45] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:45,987 [root] INFO: Process with pid 2960 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:52] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

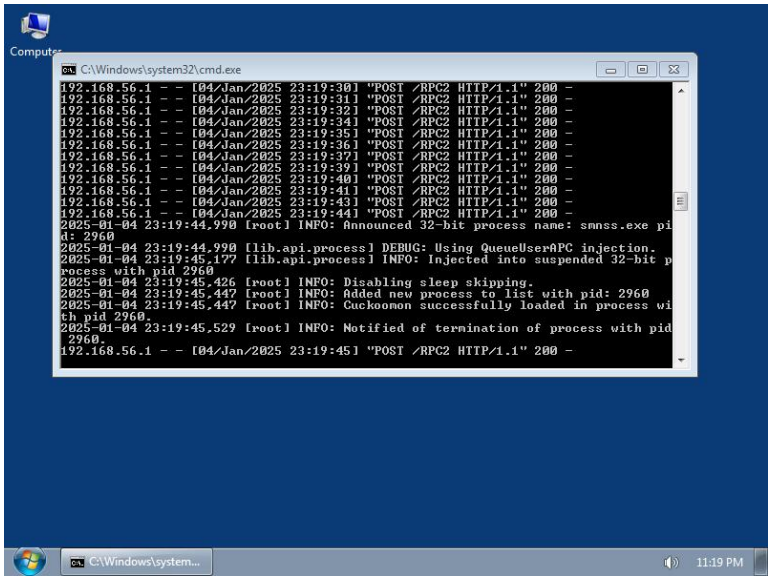

C:\Windows\system32\cmd.exe
2025-01-04 23:19:27,625 [modules.auxiliary.human] INFO: Found button "Close the
program", clicking it
192.168.56.1 - - [04/Jan/2025 23:19:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:29] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:29,177 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2760
2025-01-04 23:19:29,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:29,516 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2760
2025-01-04 23:19:29,573 [root] INFO: Notified of termination of process with pid
 2536.
2025-01-04 23:19:29,838 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:29,933 [root] INFO: Added new process to list with pid: 2760
2025-01-04 23:19:29,933 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2760.
2025-01-04 23:19:30,424 [root] INFO: Process with pid 2536 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:39] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

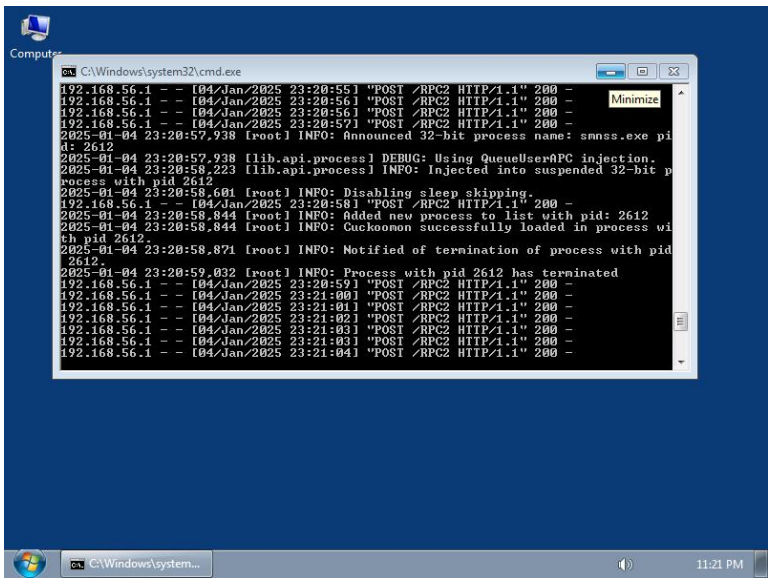

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:22:14,743 [root] INFO: Notified of termination of process with pid
540.
2025-01-04 23:22:15,371 [root] INFO: Process with pid 540 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:26,776 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3016
2025-01-04 23:22:26,776 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:26,891 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3016
2025-01-04 23:22:26,911 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:26,930 [root] INFO: Added new process to list with pid: 3016
2025-01-04 23:22:26,930 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3016.
2025-01-04 23:22:26,930 [root] INFO: Notified of termination of process with pid
3016.
C:\Windows\system...
11:22 PM

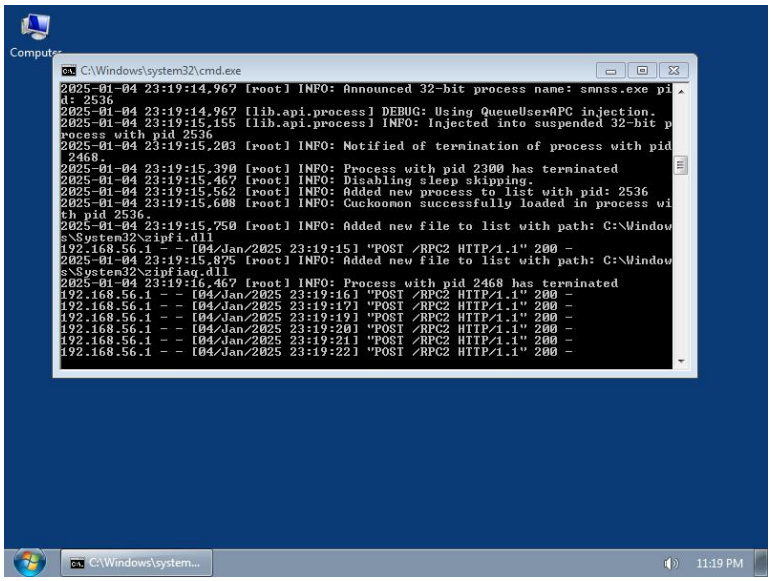

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:20:27,931 [root] INFO: Process with pid 2312 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:37] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,006 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2620
2025-01-04 23:20:38,006 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:38,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2620
192.168.56.1 - - [04/Jan/2025 23:20:38] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,240 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:38,341 [root] INFO: Added new process to list with pid: 2620
2025-01-04 23:20:38,341 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2620.
2025-01-04 23:20:38,440 [root] INFO: Notified of termination of process with pid
2620.
2025-01-04 23:20:38,823 [root] INFO: Process with pid 2620 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:40] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

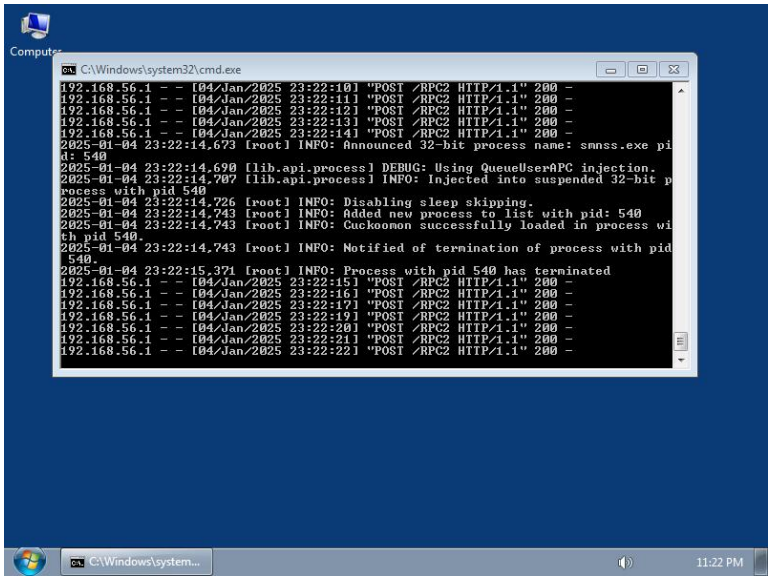

Computer
C:\Windows\system32\cmd.exe
2312.
192.168.56.1 - - [04/Jan/2025 23:20:27] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:27,931 [root] INFO: Process with pid 2312 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:37] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,006 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2620
2025-01-04 23:20:38,006 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:38,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2620
192.168.56.1 - - [04/Jan/2025 23:20:38] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,240 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:38,341 [root] INFO: Added new process to list with pid: 2620
2025-01-04 23:20:38,341 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2620.
2025-01-04 23:20:38,440 [root] INFO: Notified of termination of process with pid
2620.
2025-01-04 23:20:38,823 [root] INFO: Process with pid 2620 has terminated
C:\Windows\system...
11:20 PM

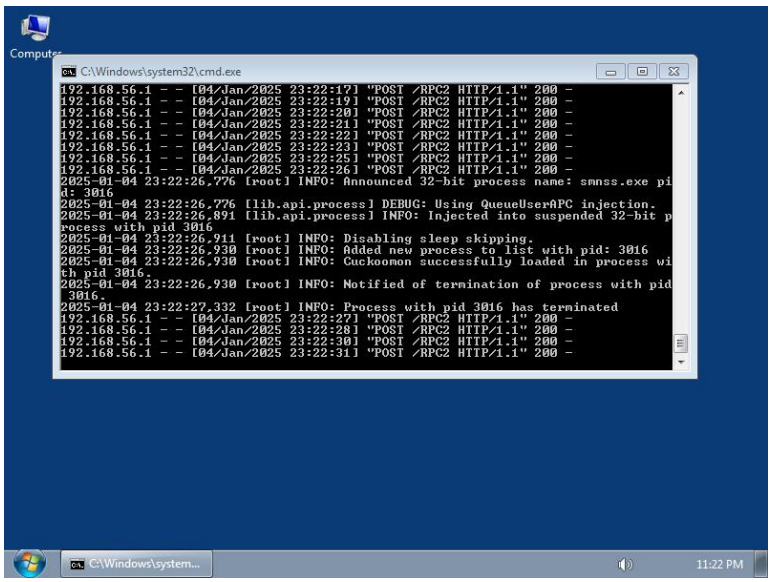

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:14,673 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 540
2025-01-04 23:22:14,690 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:14,707 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 540
2025-01-04 23:22:14,726 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:14,743 [root] INFO: Added new process to list with pid: 540
2025-01-04 23:22:14,743 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 540.
2025-01-04 23:22:14,743 [root] INFO: Notified of termination of process with pid
 540.
2025-01-04 23:22:15,371 [root] INFO: Process with pid 540 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:20] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

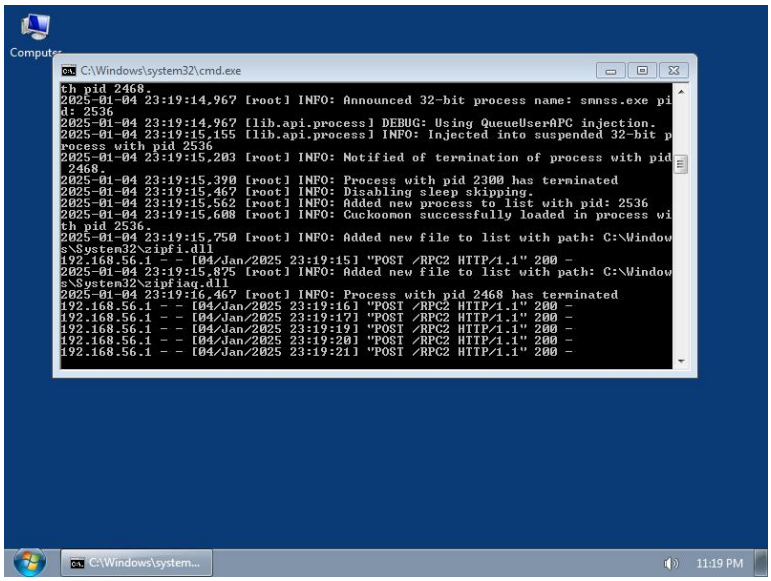

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:44] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:44,990 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2960
2025-01-04 23:19:44,990 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:45,177 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2960
2025-01-04 23:19:45,426 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:45,447 [root] INFO: Added new process to list with pid: 2960
2025-01-04 23:19:45,447 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2960.
2025-01-04 23:19:45,529 [root] INFO: Notified of termination of process with pid
 2960.
192.168.56.1 - - [04/Jan/2025 23:19:45] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

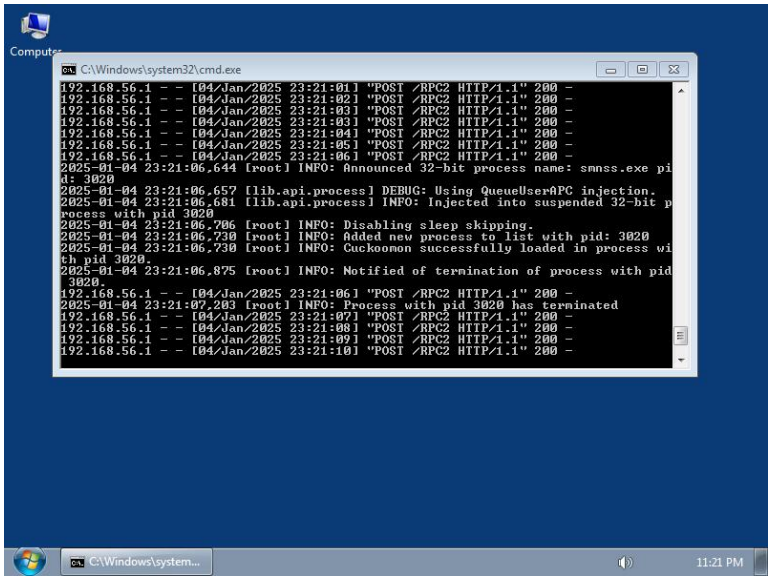

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:57] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:57,938 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2612
2025-01-04 23:20:57,938 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:58,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2612
2025-01-04 23:20:58,601 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [04/Jan/2025 23:20:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:58,844 [root] INFO: Added new process to list with pid: 2612
2025-01-04 23:20:58,844 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2612.
2025-01-04 23:20:58,871 [root] INFO: Notified of termination of process with pid
 2612.
2025-01-04 23:20:59,032 [root] INFO: Process with pid 2612 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:04] "POST /RPC2 HTTP/1.1" 200 -
Minimize
C:\Windows\system...
11:21 PM

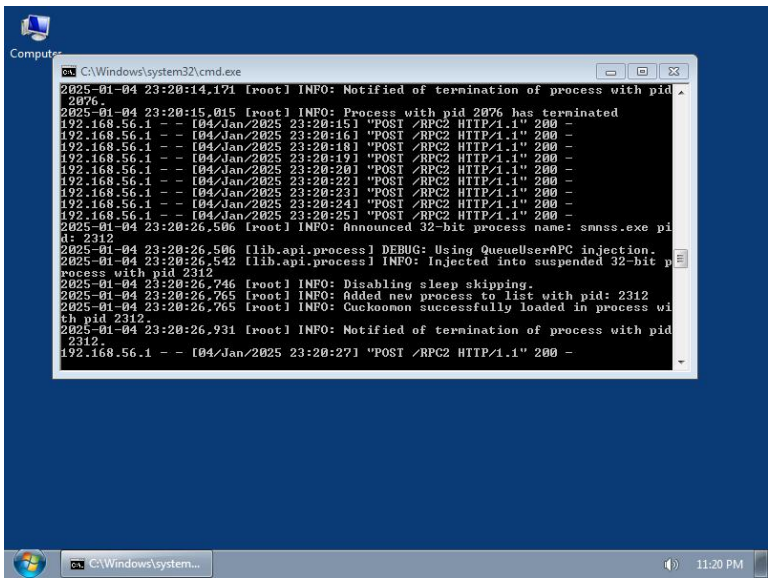

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:19:14,967 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2536
2025-01-04 23:19:14,967 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:15,155 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2536
2025-01-04 23:19:15,203 [root] INFO: Notified of termination of process with pid 2468.
2025-01-04 23:19:15,390 [root] INFO: Process with pid 2300 has terminated
2025-01-04 23:19:15,467 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:15,562 [root] INFO: Added new process to list with pid: 2536
2025-01-04 23:19:15,608 [root] INFO: Cuckoomon successfully loaded in process with pid 2536.
2025-01-04 23:19:15,750 [root] INFO: Added new file to list with path: C:\Windows\System32\zipfi.dll
192.168.56.1 - - [04/Jan/2025 23:19:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:15,875 [root] INFO: Added new file to list with path: C:\Windows\System32\zipfiaq.dll
2025-01-04 23:19:16,467 [root] INFO: Process with pid 2468 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:22] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

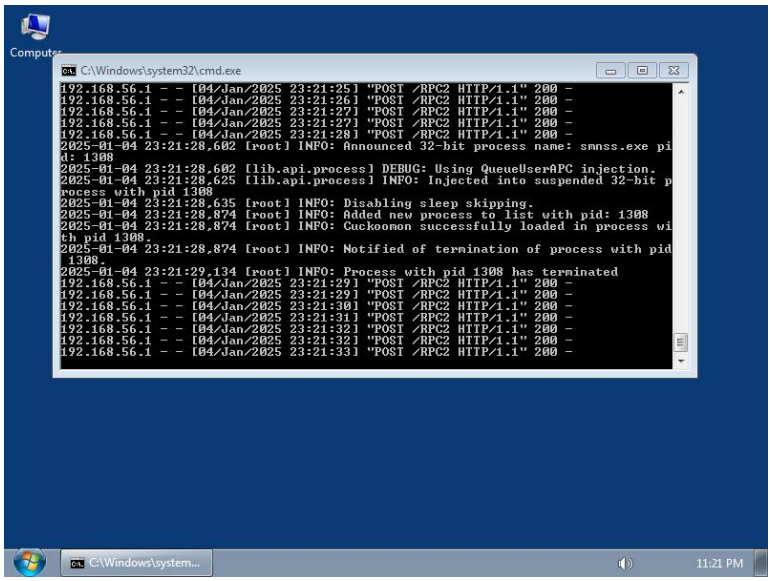

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:14,673 [root] INFO: Announced 32-bit process name: smnss.exe pid: 540
2025-01-04 23:22:14,690 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:14,707 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 540
2025-01-04 23:22:14,726 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:14,743 [root] INFO: Added new process to list with pid: 540
2025-01-04 23:22:14,743 [root] INFO: Cuckoomon successfully loaded in process with pid 540.
2025-01-04 23:22:14,743 [root] INFO: Notified of termination of process with pid 540.
2025-01-04 23:22:15,371 [root] INFO: Process with pid 540 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:22] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

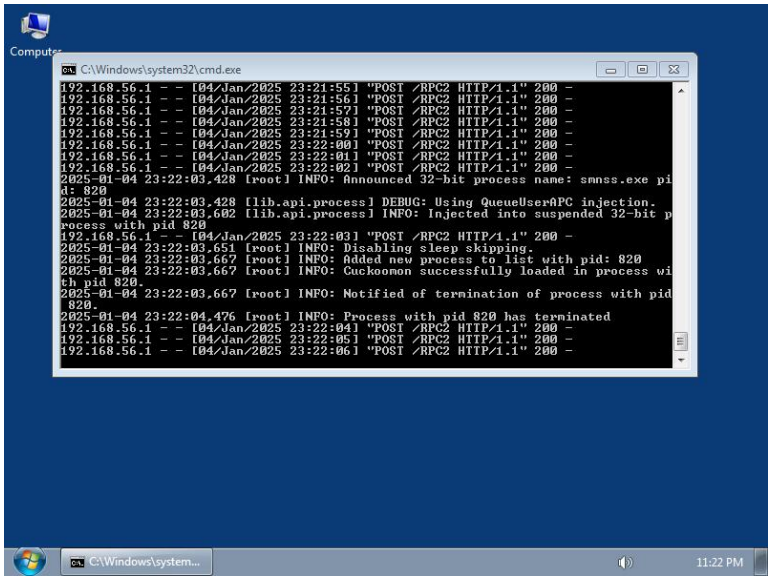

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:26,776 [root] INFO: Announced 32-bit process name: smnss.exe pid: 3016
2025-01-04 23:22:26,776 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:26,891 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 3016
2025-01-04 23:22:26,911 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:26,930 [root] INFO: Added new process to list with pid: 3016
2025-01-04 23:22:26,930 [root] INFO: Cuckoomon successfully loaded in process with pid 3016.
2025-01-04 23:22:26,930 [root] INFO: Notified of termination of process with pid 3016.
2025-01-04 23:22:27,332 [root] INFO: Process with pid 3016 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:31] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

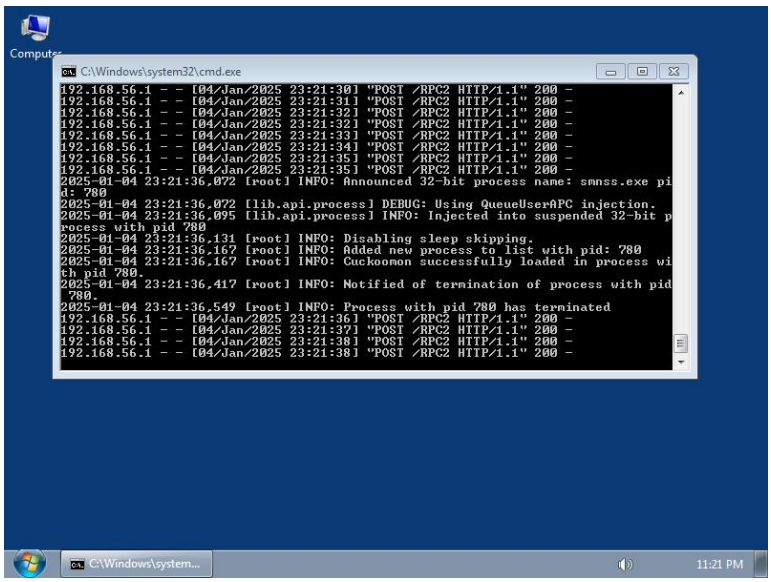

Computer
C:\Windows\system32\cmd.exe
th pid 2468.
2025-01-04 23:19:14,967 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2536
2025-01-04 23:19:14,967 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:15,155 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2536
2025-01-04 23:19:15,203 [root] INFO: Notified of termination of process with pid
2468.
2025-01-04 23:19:15,390 [root] INFO: Process with pid 2300 has terminated
2025-01-04 23:19:15,467 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:15,562 [root] INFO: Added new process to list with pid: 2536
2025-01-04 23:19:15,608 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2536.
2025-01-04 23:19:15,750 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfi.dll
192.168.56.1 - - [04/Jan/2025 23:19:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:15,875 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfiaq.dll
2025-01-04 23:19:16,467 [root] INFO: Process with pid 2468 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:21] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

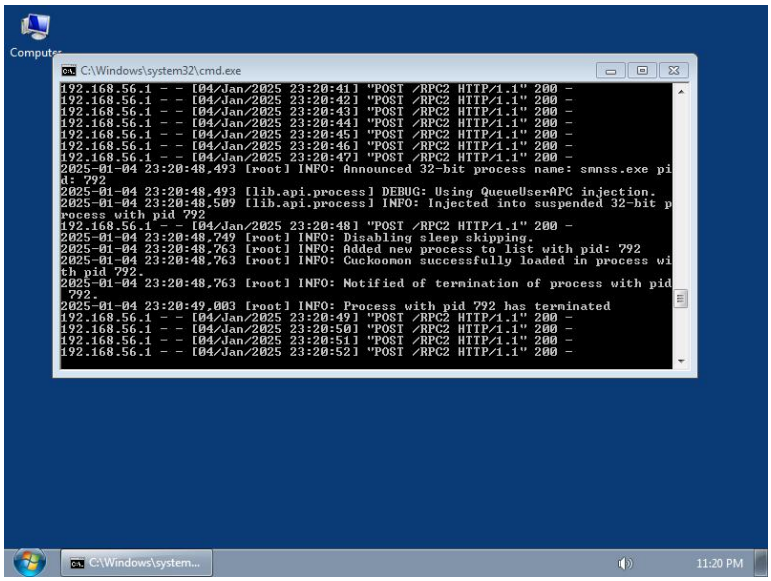

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:06,644 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3020
2025-01-04 23:21:06,657 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:06,681 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3020
2025-01-04 23:21:06,706 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:06,730 [root] INFO: Added new process to list with pid: 3020
2025-01-04 23:21:06,730 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3020.
2025-01-04 23:21:06,875 [root] INFO: Notified of termination of process with pid
3020.
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:07,203 [root] INFO: Process with pid 3020 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

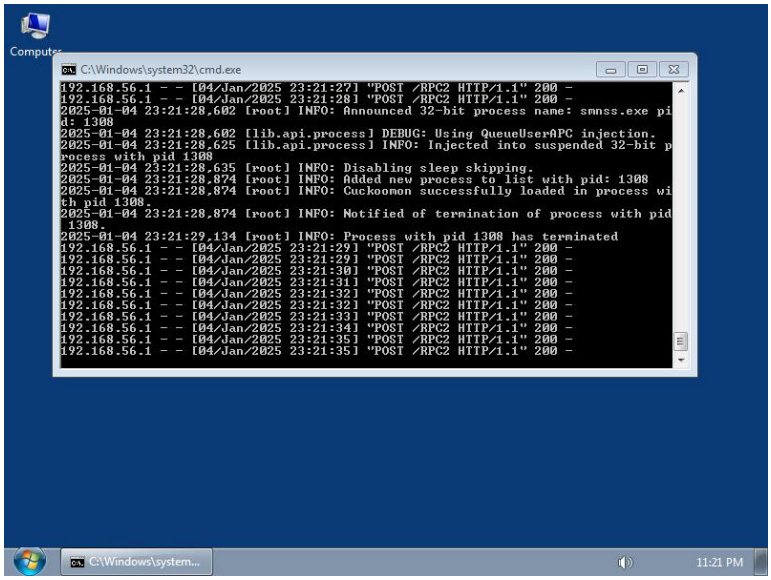

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:20:14,171 [root] INFO: Notified of termination of process with pid
2076.
2025-01-04 23:20:15,015 [root] INFO: Process with pid 2076 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:25] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:26,506 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2312
2025-01-04 23:20:26,506 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:26,542 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2312
2025-01-04 23:20:26,746 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:26,765 [root] INFO: Added new process to list with pid: 2312
2025-01-04 23:20:26,765 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2312.
2025-01-04 23:20:26,931 [root] INFO: Notified of termination of process with pid
2312.
192.168.56.1 - - [04/Jan/2025 23:20:27] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

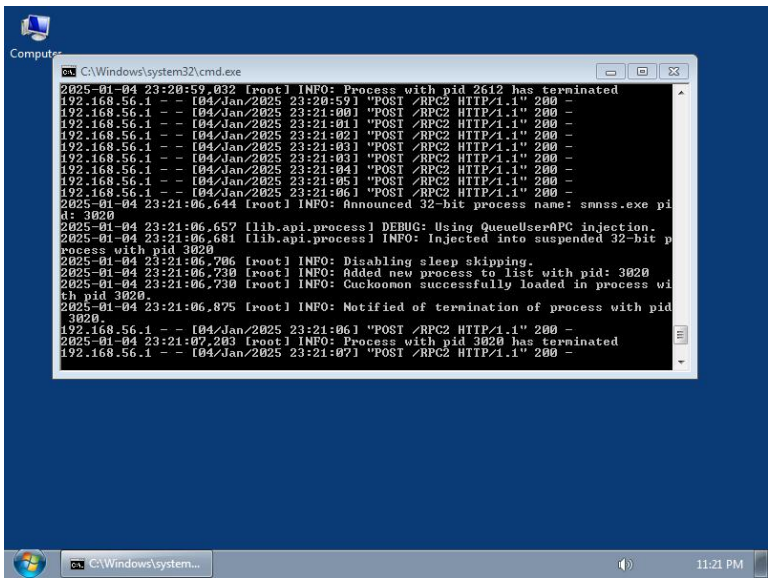

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:28] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:28,602 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1308
2025-01-04 23:21:28,602 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:28,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1308
2025-01-04 23:21:28,635 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:28,874 [root] INFO: Added new process to list with pid: 1308
2025-01-04 23:21:28,874 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1308.
2025-01-04 23:21:28,874 [root] INFO: Notified of termination of process with pid
 1308.
2025-01-04 23:21:29,134 [root] INFO: Process with pid 1308 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:33] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

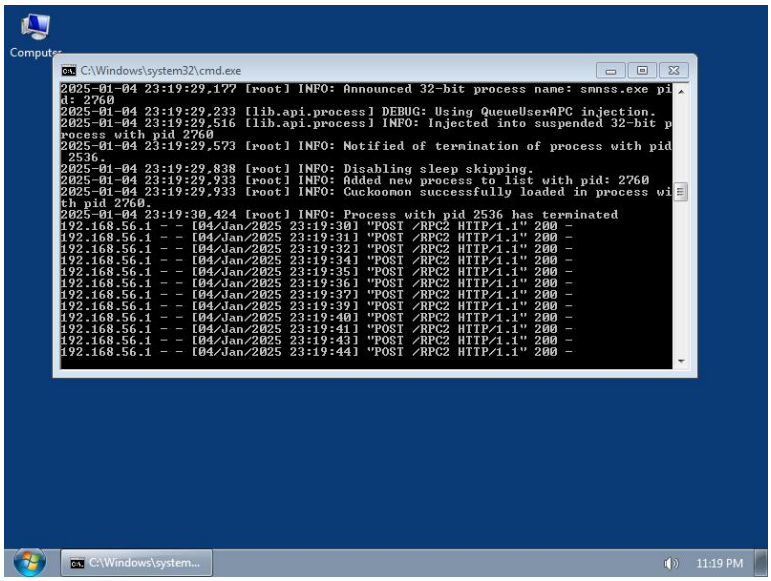

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:02] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,428 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 820
2025-01-04 23:22:03,428 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:03,602 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 820
192.168.56.1 - - [04/Jan/2025 23:22:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,651 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:03,667 [root] INFO: Added new process to list with pid: 820
2025-01-04 23:22:03,667 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 820.
2025-01-04 23:22:03,667 [root] INFO: Notified of termination of process with pid
 820.
2025-01-04 23:22:04,476 [root] INFO: Process with pid 820 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:06] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

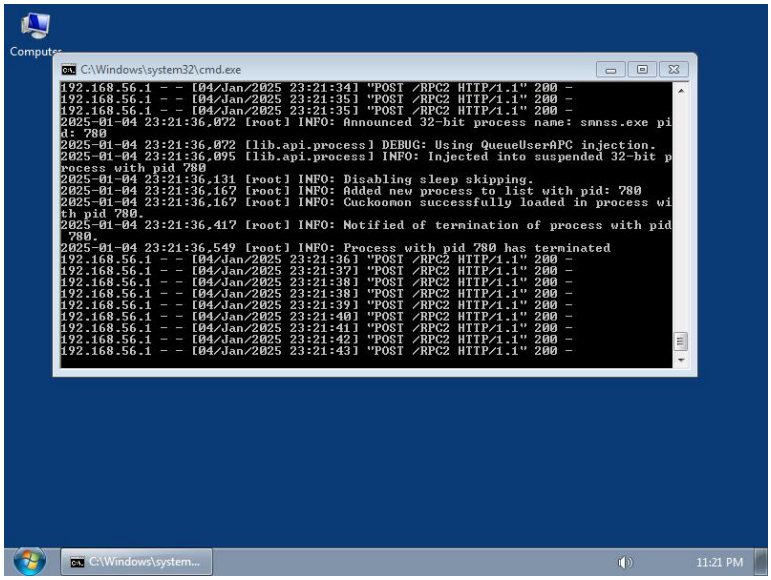

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:36,072 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 780
2025-01-04 23:21:36,072 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:36,095 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 780
2025-01-04 23:21:36,131 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:36,167 [root] INFO: Added new process to list with pid: 780
2025-01-04 23:21:36,167 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 780.
2025-01-04 23:21:36,417 [root] INFO: Notified of termination of process with pid
 780.
2025-01-04 23:21:36,549 [root] INFO: Process with pid 780 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

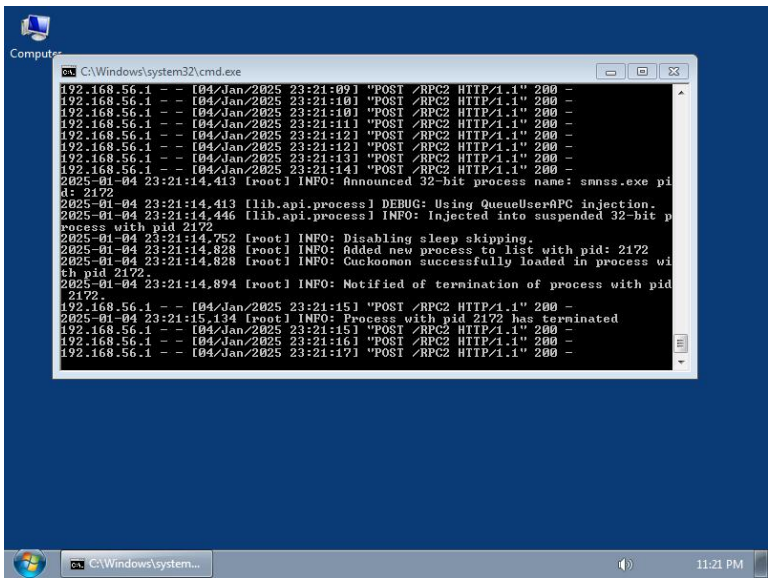

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:47] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,493 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 792
2025-01-04 23:20:48,493 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:48,509 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 792
192.168.56.1 - - [04/Jan/2025 23:20:48] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,749 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:48,763 [root] INFO: Added new process to list with pid: 792
2025-01-04 23:20:48,763 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 792.
2025-01-04 23:20:48,763 [root] INFO: Notified of termination of process with pid
 792.
2025-01-04 23:20:49,003 [root] INFO: Process with pid 792 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:52] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

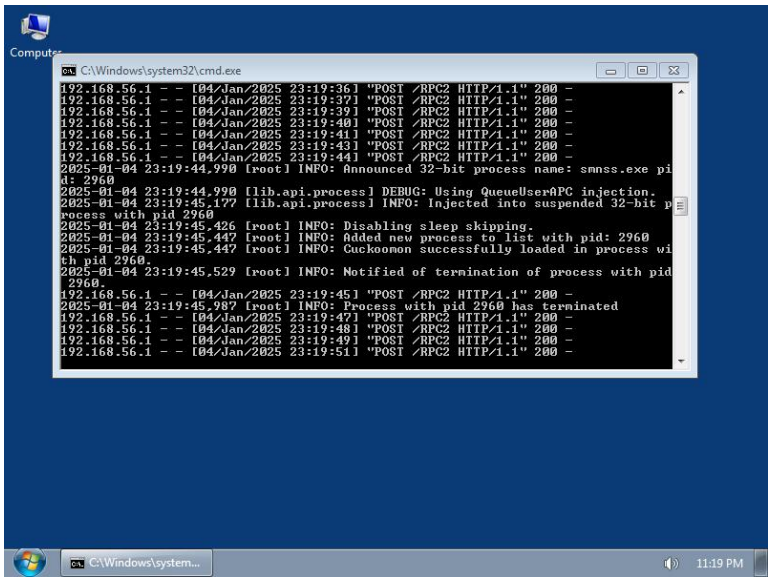

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:28] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:28,602 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1308
2025-01-04 23:21:28,602 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:28,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1308
2025-01-04 23:21:28,635 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:28,874 [root] INFO: Added new process to list with pid: 1308
2025-01-04 23:21:28,874 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1308.
2025-01-04 23:21:28,874 [root] INFO: Notified of termination of process with pid
 1308.
2025-01-04 23:21:29,134 [root] INFO: Process with pid 1308 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

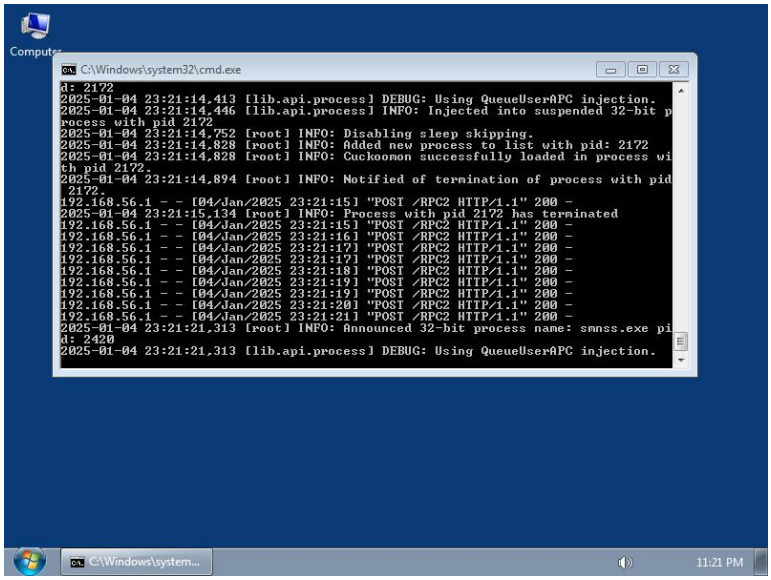

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:20:59,032 [root] INFO: Process with pid 2612 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:06,644 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3020
2025-01-04 23:21:06,657 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:06,681 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3020
2025-01-04 23:21:06,706 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:06,730 [root] INFO: Added new process to list with pid: 3020
2025-01-04 23:21:06,730 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3020.
2025-01-04 23:21:06,875 [root] INFO: Notified of termination of process with pid
 3020.
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:07,203 [root] INFO: Process with pid 3020 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:07] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

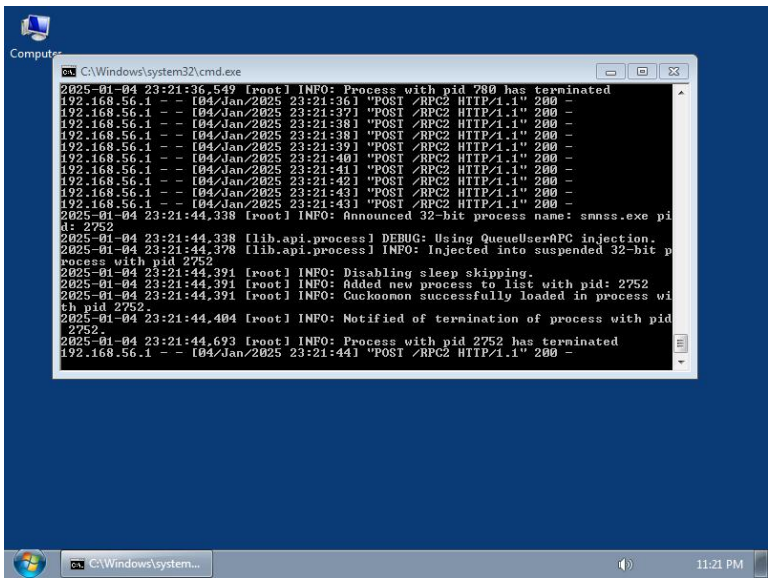

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:19:29,177 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2760
2025-01-04 23:19:29,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:29,516 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2760
2025-01-04 23:19:29,573 [root] INFO: Notified of termination of process with pid 2536.
2025-01-04 23:19:29,838 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:29,933 [root] INFO: Added new process to list with pid: 2760
2025-01-04 23:19:29,933 [root] INFO: Cuckoomon successfully loaded in process with pid 2760.
2025-01-04 23:19:30,424 [root] INFO: Process with pid 2536 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:44] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

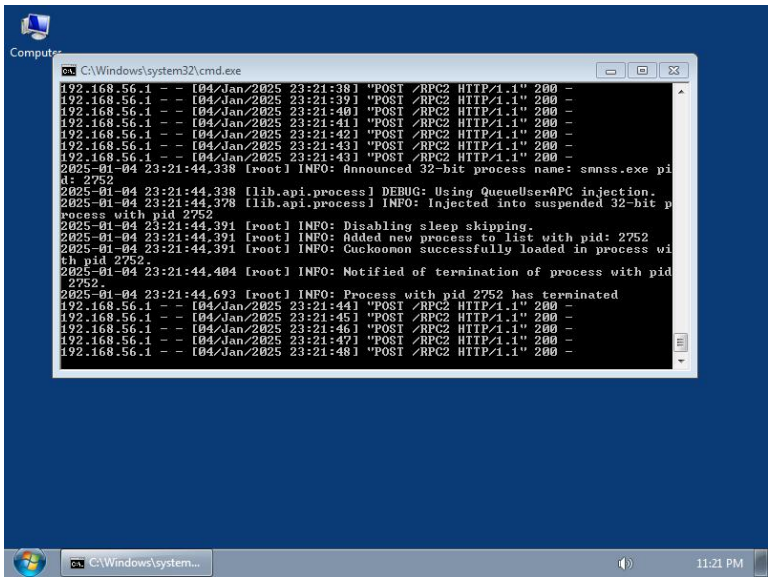

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:36,072 [root] INFO: Announced 32-bit process name: smnss.exe pid: 780
2025-01-04 23:21:36,072 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:36,095 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 780
2025-01-04 23:21:36,131 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:36,167 [root] INFO: Added new process to list with pid: 780
2025-01-04 23:21:36,167 [root] INFO: Cuckoomon successfully loaded in process with pid 780.
2025-01-04 23:21:36,417 [root] INFO: Notified of termination of process with pid 780.
2025-01-04 23:21:36,549 [root] INFO: Process with pid 780 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

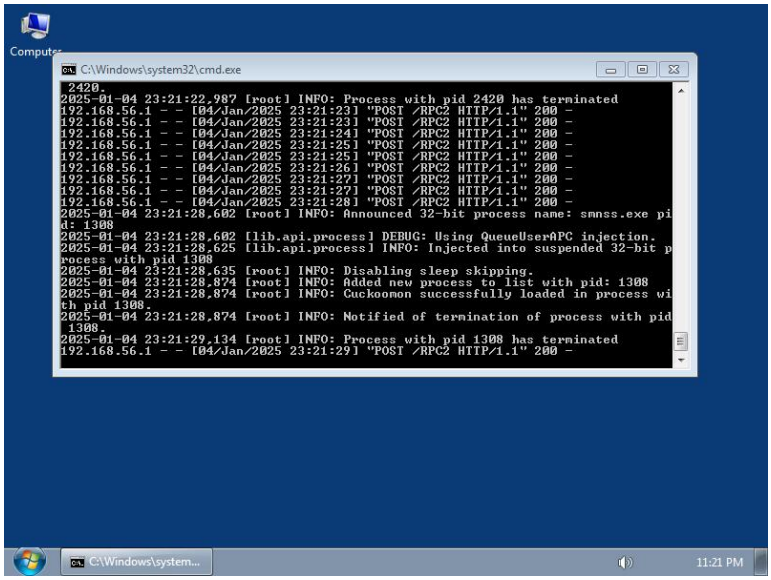

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:14,413 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2172
2025-01-04 23:21:14,413 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:14,446 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2172
2025-01-04 23:21:14,752 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:14,828 [root] INFO: Added new process to list with pid: 2172
2025-01-04 23:21:14,828 [root] INFO: Cuckoomon successfully loaded in process with pid 2172.
2025-01-04 23:21:14,894 [root] INFO: Notified of termination of process with pid 2172.
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:15,134 [root] INFO: Process with pid 2172 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

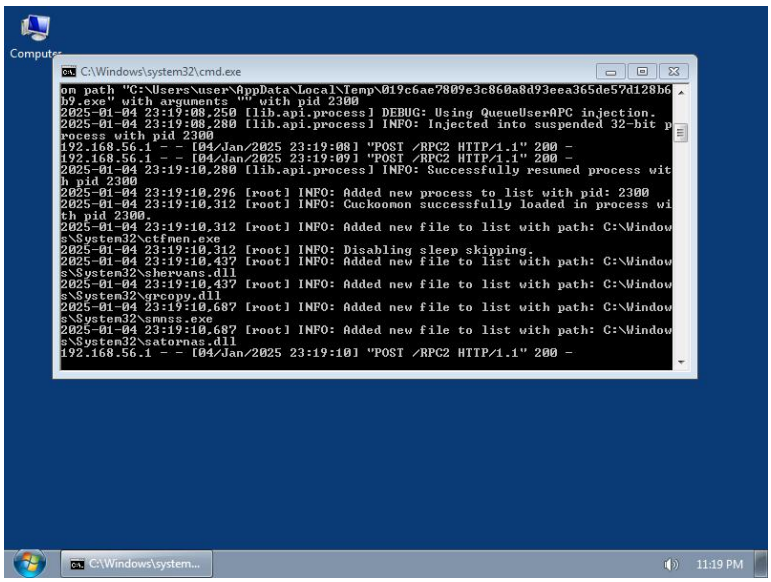

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:44] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:44,990 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2960
2025-01-04 23:19:44,990 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:45,177 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2960
2025-01-04 23:19:45,426 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:45,447 [root] INFO: Added new process to list with pid: 2960
2025-01-04 23:19:45,447 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2960.
2025-01-04 23:19:45,529 [root] INFO: Notified of termination of process with pid
 2960.
192.168.56.1 - - [04/Jan/2025 23:19:45] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:45,987 [root] INFO: Process with pid 2960 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:51] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

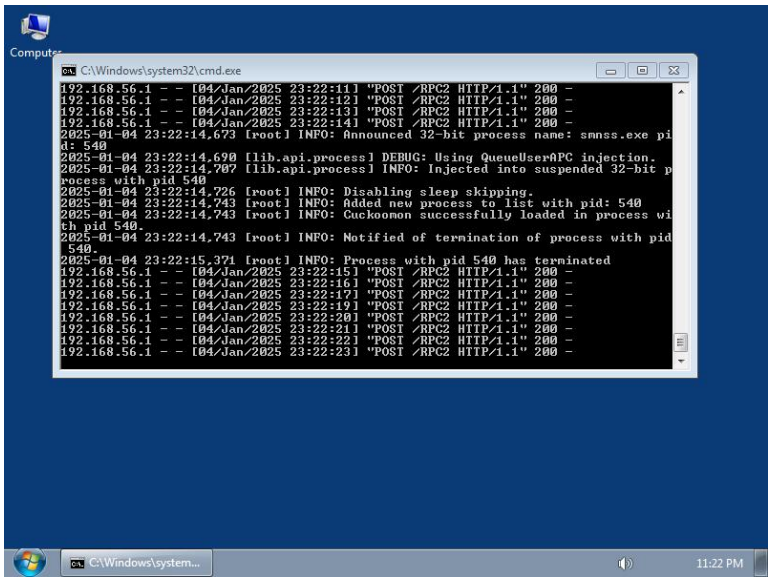

Computer
C:\Windows\system32\cmd.exe
d: 2172
2025-01-04 23:21:14,413 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:14,446 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2172
2025-01-04 23:21:14,752 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:14,828 [root] INFO: Added new process to list with pid: 2172
2025-01-04 23:21:14,828 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2172.
2025-01-04 23:21:14,894 [root] INFO: Notified of termination of process with pid
 2172.
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:15,134 [root] INFO: Process with pid 2172 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,313 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2420
2025-01-04 23:21:21,313 [lib.api.process] DEBUG: Using QueueUserAPC injection.
C:\Windows\system...
11:21 PM

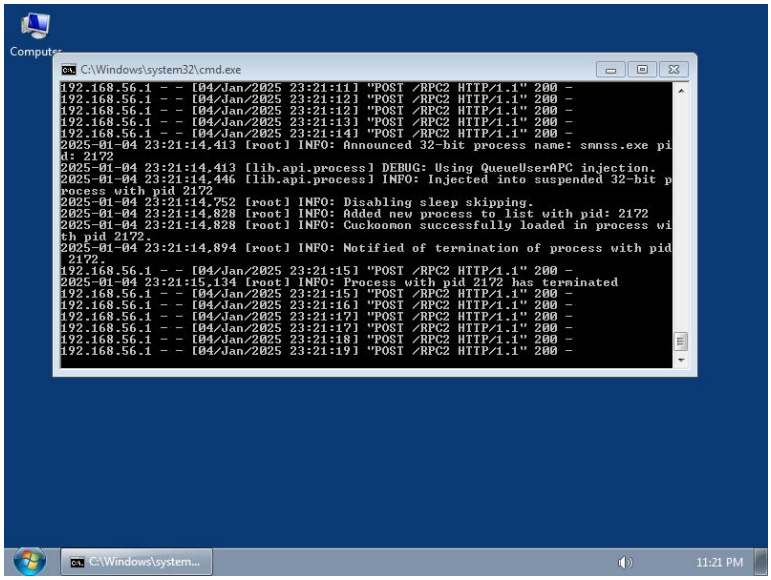

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:21:36,549 [root] INFO: Process with pid 780 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:44,338 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2752
2025-01-04 23:21:44,338 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:44,378 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2752
2025-01-04 23:21:44,391 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:44,391 [root] INFO: Added new process to list with pid: 2752
2025-01-04 23:21:44,391 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2752.
2025-01-04 23:21:44,404 [root] INFO: Notified of termination of process with pid
 2752.
2025-01-04 23:21:44,693 [root] INFO: Process with pid 2752 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:44] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

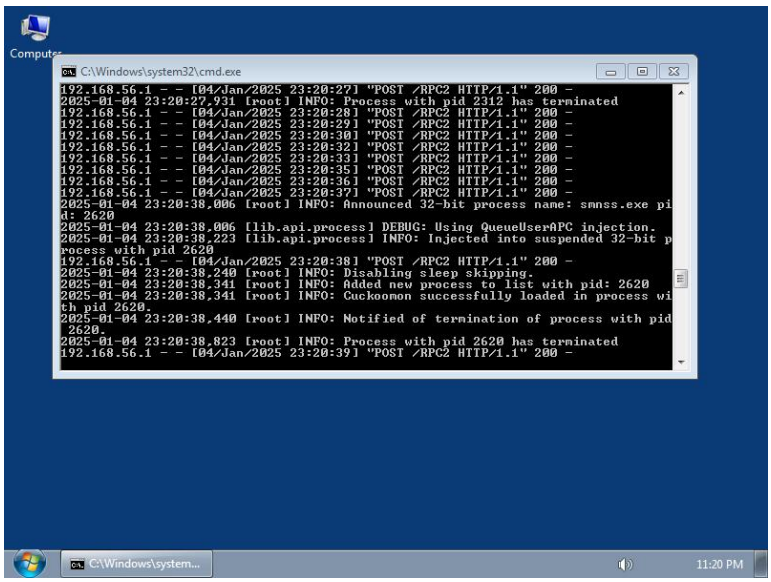

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:44,338 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2752
2025-01-04 23:21:44,338 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:44,378 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2752
2025-01-04 23:21:44,391 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:44,391 [root] INFO: Added new process to list with pid: 2752
2025-01-04 23:21:44,391 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2752.
2025-01-04 23:21:44,404 [root] INFO: Notified of termination of process with pid
 2752.
2025-01-04 23:21:44,693 [root] INFO: Process with pid 2752 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:48] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

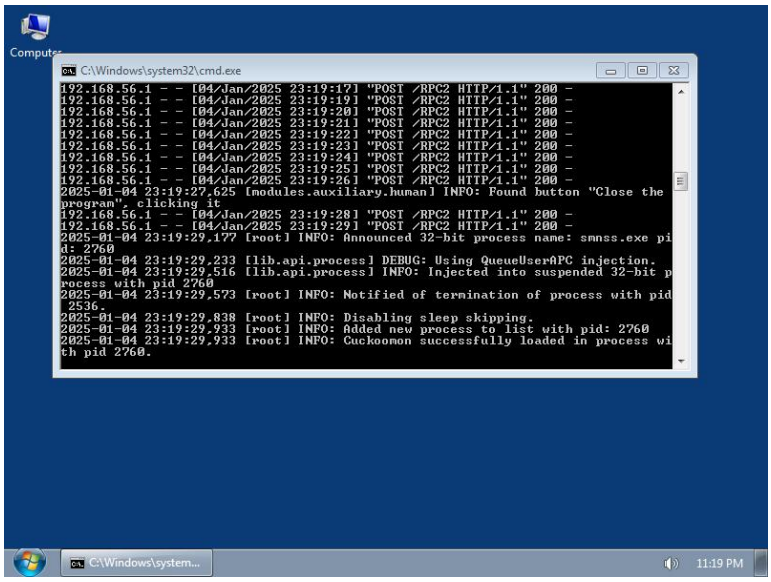

Computer
C:\Windows\system32\cmd.exe
 2420.
2025-01-04 23:21:22,987 [root] INFO: Process with pid 2420 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:28] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:28,602 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1308
2025-01-04 23:21:28,602 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:28,625 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1308
2025-01-04 23:21:28,635 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:28,874 [root] INFO: Added new process to list with pid: 1308
2025-01-04 23:21:28,874 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1308.
2025-01-04 23:21:28,874 [root] INFO: Notified of termination of process with pid
 1308.
2025-01-04 23:21:29,134 [root] INFO: Process with pid 1308 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:29] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

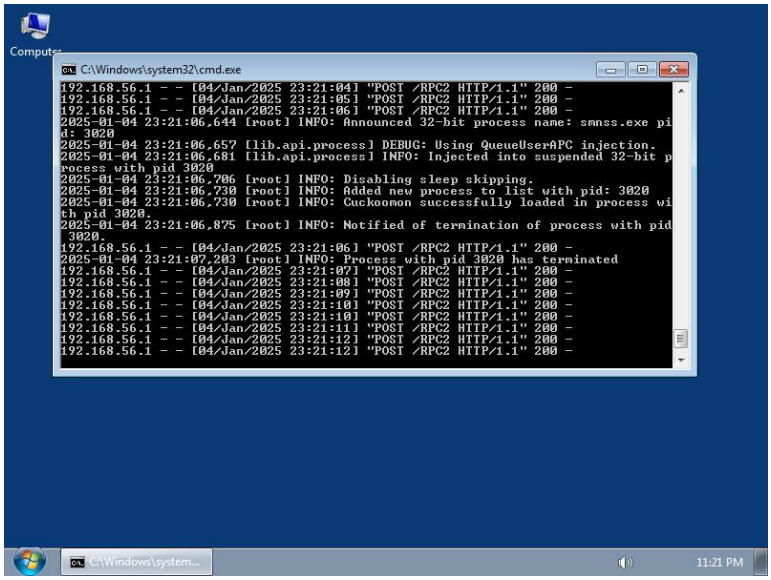

Computer
C:\Windows\system32\cmd.exe
on path "C:\Users\user\AppData\Local\Temp\019c6ae7809e3c860a8d93eea365de57d128b6
b9.exe" with arguments "" with pid 2300
2025-01-04 23:19:08,250 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:08,280 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2300
192.168.56.1 - - [04/Jan/2025 23:19:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:09] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:10,280 [lib.api.process] INFO: Successfully resumed process wit
h pid 2300
2025-01-04 23:19:10,296 [root] INFO: Added new process to list with pid: 2300
2025-01-04 23:19:10,312 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2300.
2025-01-04 23:19:10,312 [root] INFO: Added new file to list with path: C:\Window
s\System32\ctfmen.exe
2025-01-04 23:19:10,312 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:10,437 [root] INFO: Added new file to list with path: C:\Window
s\System32\shervans.dll
2025-01-04 23:19:10,437 [root] INFO: Added new file to list with path: C:\Window
s\System32\grcopy.dll
2025-01-04 23:19:10,687 [root] INFO: Added new file to list with path: C:\Window
s\System32\smnss.exe
2025-01-04 23:19:10,687 [root] INFO: Added new file to list with path: C:\Window
s\System32\satornas.dll
192.168.56.1 - - [04/Jan/2025 23:19:10] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

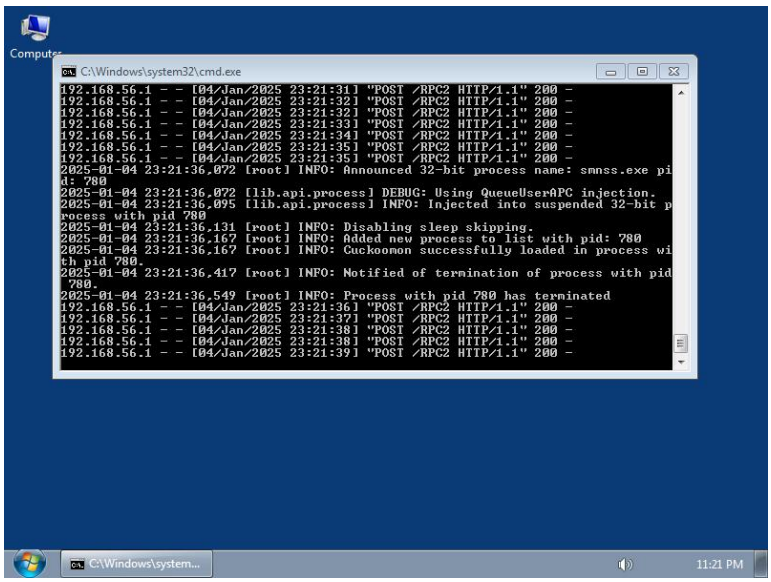

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:14,673 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 540
2025-01-04 23:22:14,690 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:14,707 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 540
2025-01-04 23:22:14,726 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:14,743 [root] INFO: Added new process to list with pid: 540
2025-01-04 23:22:14,743 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 540.
2025-01-04 23:22:14,743 [root] INFO: Notified of termination of process with pid
 540.
2025-01-04 23:22:15,371 [root] INFO: Process with pid 540 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:23] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

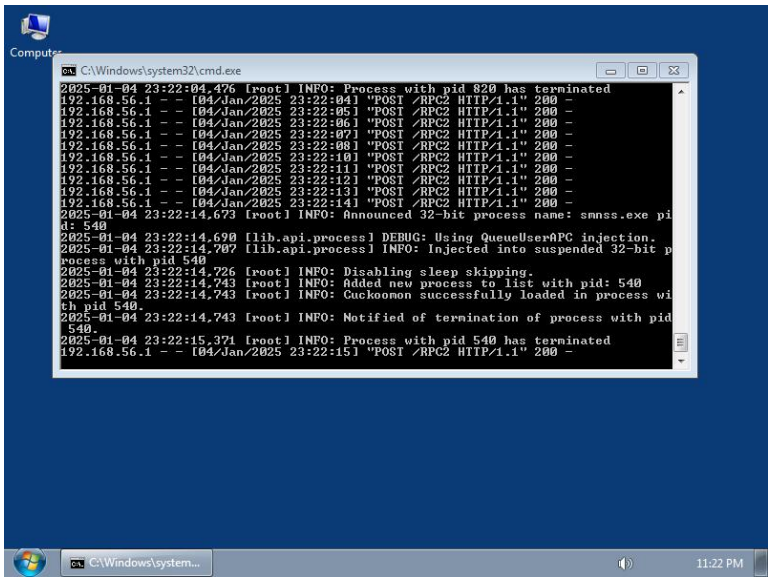

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:14,413 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2172
2025-01-04 23:21:14,413 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:14,446 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2172
2025-01-04 23:21:14,752 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:14,828 [root] INFO: Added new process to list with pid: 2172
2025-01-04 23:21:14,828 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2172.
2025-01-04 23:21:14,894 [root] INFO: Notified of termination of process with pid
 2172.
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:15,134 [root] INFO: Process with pid 2172 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

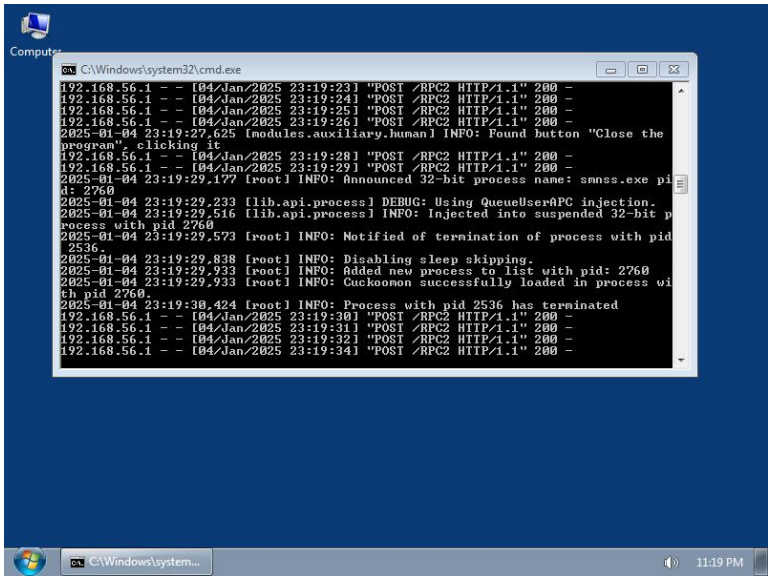

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:27] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:27,931 [root] INFO: Process with pid 2312 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:37] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,006 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2620
2025-01-04 23:20:38,006 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:38,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2620
192.168.56.1 - - [04/Jan/2025 23:20:38] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,240 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:38,341 [root] INFO: Added new process to list with pid: 2620
2025-01-04 23:20:38,341 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2620.
2025-01-04 23:20:38,440 [root] INFO: Notified of termination of process with pid
 2620.
2025-01-04 23:20:38,823 [root] INFO: Process with pid 2620 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:39] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

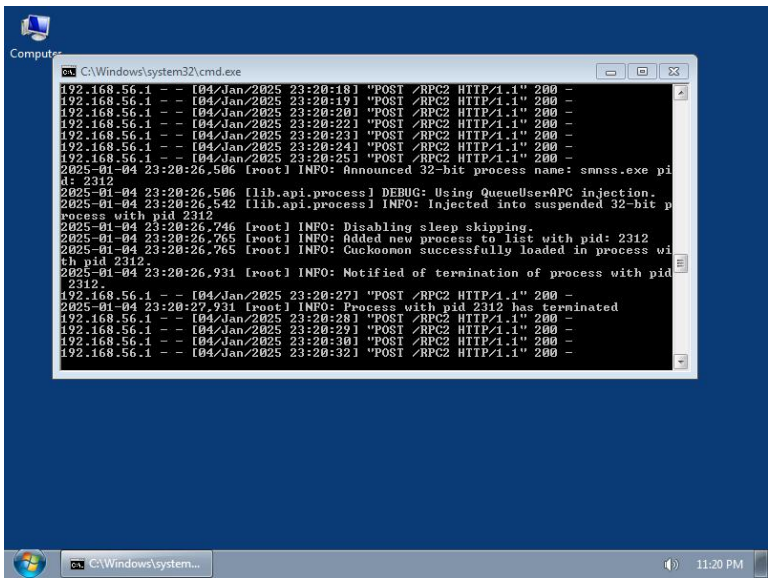

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:27,625 [modules.auxiliary.human] INFO: Found button "Close the program", clicking it
192.168.56.1 - - [04/Jan/2025 23:19:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:29] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:29,177 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2760
2025-01-04 23:19:29,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:29,516 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2760
2025-01-04 23:19:29,573 [root] INFO: Notified of termination of process with pid 2536.
2025-01-04 23:19:29,838 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:29,933 [root] INFO: Added new process to list with pid: 2760
2025-01-04 23:19:29,933 [root] INFO: Cuckoomon successfully loaded in process with pid 2760.
C:\Windows\system...
11:19 PM

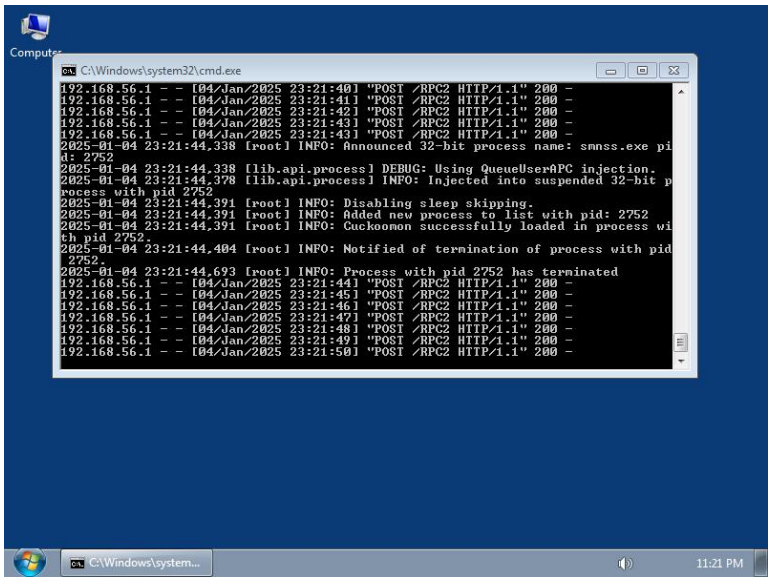

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:06,644 [root] INFO: Announced 32-bit process name: smnss.exe pid: 3020
2025-01-04 23:21:06,657 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:06,681 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 3020
2025-01-04 23:21:06,706 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:06,730 [root] INFO: Added new process to list with pid: 3020
2025-01-04 23:21:06,730 [root] INFO: Cuckoomon successfully loaded in process with pid 3020.
2025-01-04 23:21:06,875 [root] INFO: Notified of termination of process with pid 3020.
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:07,203 [root] INFO: Process with pid 3020 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

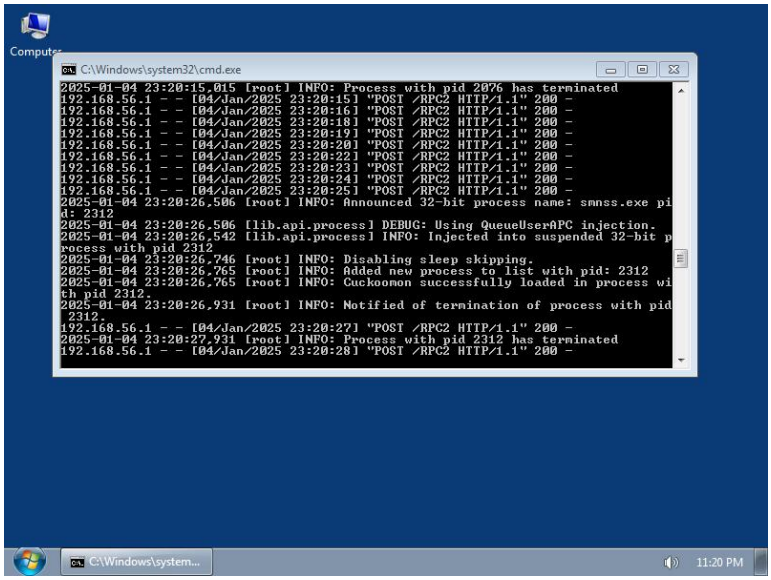

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:35] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:36,072 [root] INFO: Announced 32-bit process name: smnss.exe pid: 780
2025-01-04 23:21:36,072 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:36,095 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 780
2025-01-04 23:21:36,131 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:36,167 [root] INFO: Added new process to list with pid: 780
2025-01-04 23:21:36,167 [root] INFO: Cuckoomon successfully loaded in process with pid 780.
2025-01-04 23:21:36,417 [root] INFO: Notified of termination of process with pid 780.
2025-01-04 23:21:36,549 [root] INFO: Process with pid 780 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:39] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

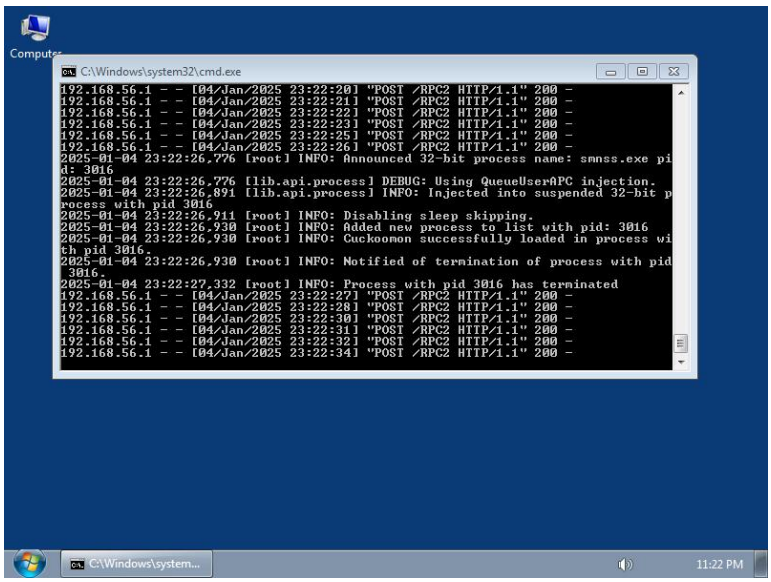

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:22:04,476 [root] INFO: Process with pid 820 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:14,673 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 540
2025-01-04 23:22:14,690 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:14,707 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 540
2025-01-04 23:22:14,726 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:14,743 [root] INFO: Added new process to list with pid: 540
2025-01-04 23:22:14,743 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 540.
2025-01-04 23:22:14,743 [root] INFO: Notified of termination of process with pid
540.
2025-01-04 23:22:15,371 [root] INFO: Process with pid 540 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:15] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

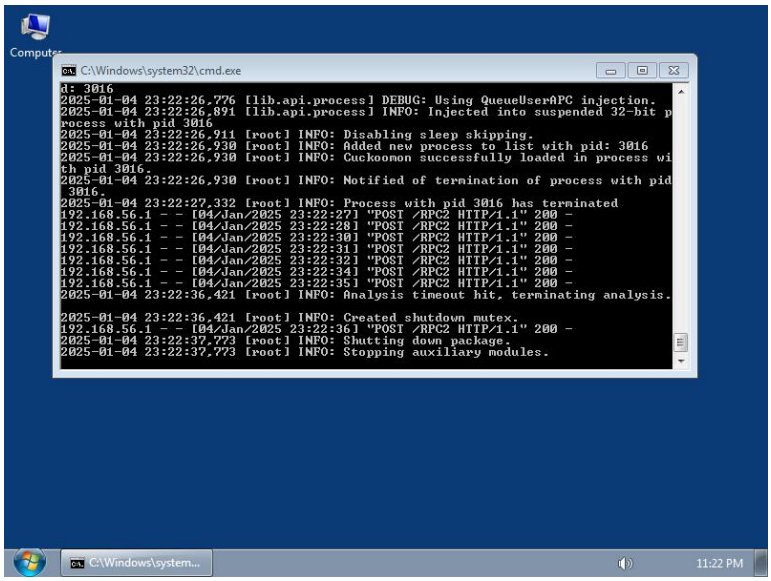

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:27,625 [modules.auxiliary.human] INFO: Found button "Close the
program", clicking it
192.168.56.1 - - [04/Jan/2025 23:19:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:29] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:29,177 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2760
2025-01-04 23:19:29,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:29,516 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2760
2025-01-04 23:19:29,573 [root] INFO: Notified of termination of process with pid
2536.
2025-01-04 23:19:29,838 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:29,933 [root] INFO: Added new process to list with pid: 2760
2025-01-04 23:19:29,933 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2760.
2025-01-04 23:19:30,424 [root] INFO: Process with pid 2536 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:34] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

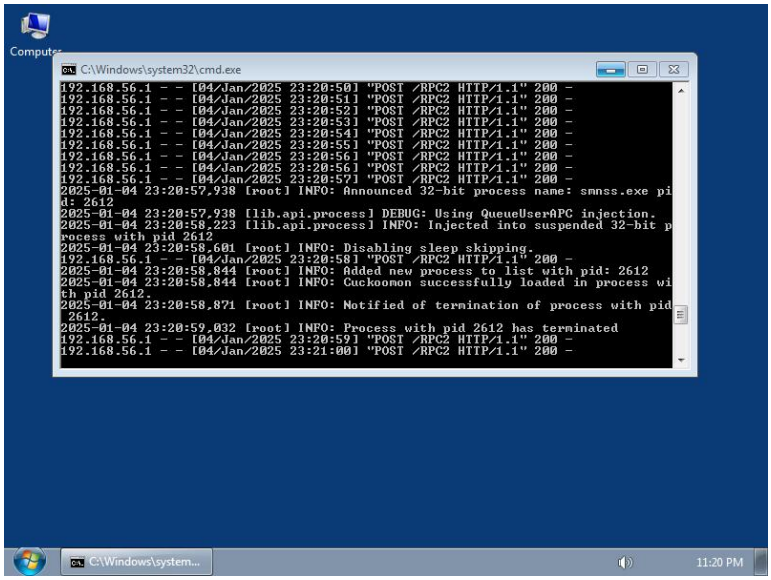

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:25] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:26,506 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2312
2025-01-04 23:20:26,506 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:26,542 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2312
2025-01-04 23:20:26,746 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:26,765 [root] INFO: Added new process to list with pid: 2312
2025-01-04 23:20:26,765 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2312.
2025-01-04 23:20:26,931 [root] INFO: Notified of termination of process with pid
2312.
192.168.56.1 - - [04/Jan/2025 23:20:27] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:27,931 [root] INFO: Process with pid 2312 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:32] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

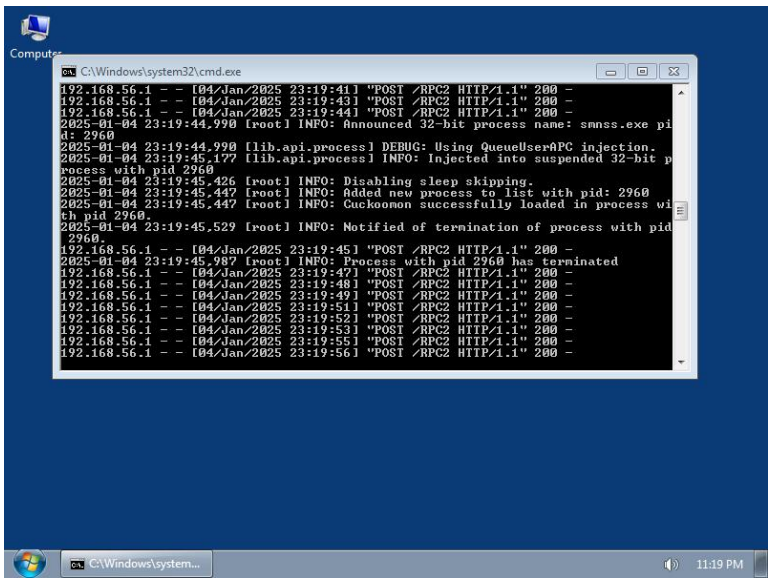

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:44,338 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2752
2025-01-04 23:21:44,338 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:44,378 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2752
2025-01-04 23:21:44,391 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:44,391 [root] INFO: Added new process to list with pid: 2752
2025-01-04 23:21:44,391 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2752.
2025-01-04 23:21:44,404 [root] INFO: Notified of termination of process with pid
 2752.
2025-01-04 23:21:44,693 [root] INFO: Process with pid 2752 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:50] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

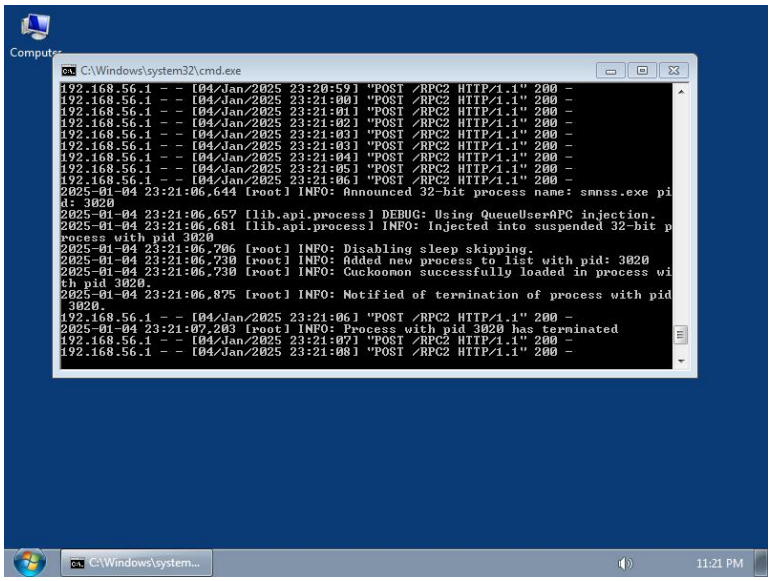

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:20:15,015 [root] INFO: Process with pid 2076 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:25] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:26,506 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2312
2025-01-04 23:20:26,506 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:26,542 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2312
2025-01-04 23:20:26,746 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:26,765 [root] INFO: Added new process to list with pid: 2312
2025-01-04 23:20:26,765 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2312.
2025-01-04 23:20:26,931 [root] INFO: Notified of termination of process with pid
 2312.
192.168.56.1 - - [04/Jan/2025 23:20:27] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:27,931 [root] INFO: Process with pid 2312 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:28] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

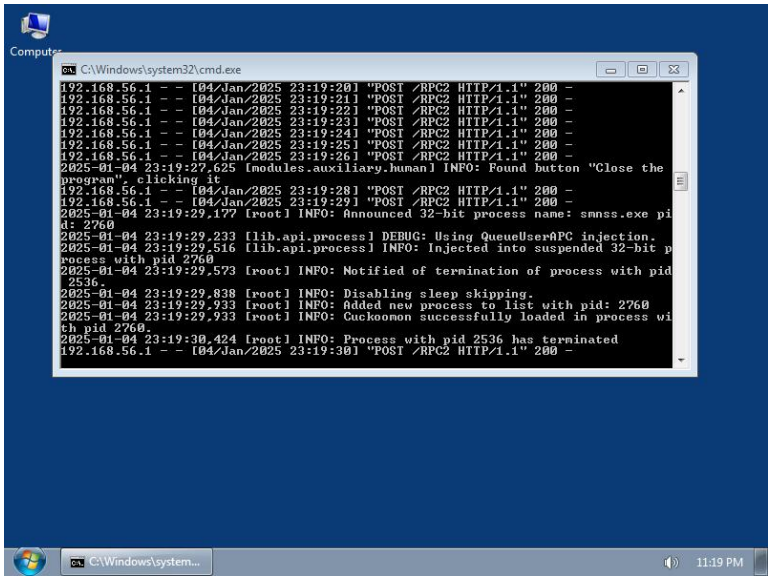

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:26,776 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3016
2025-01-04 23:22:26,776 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:26,891 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3016
2025-01-04 23:22:26,911 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:26,930 [root] INFO: Added new process to list with pid: 3016
2025-01-04 23:22:26,930 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3016.
2025-01-04 23:22:26,930 [root] INFO: Notified of termination of process with pid
 3016.
2025-01-04 23:22:27,332 [root] INFO: Process with pid 3016 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:34] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

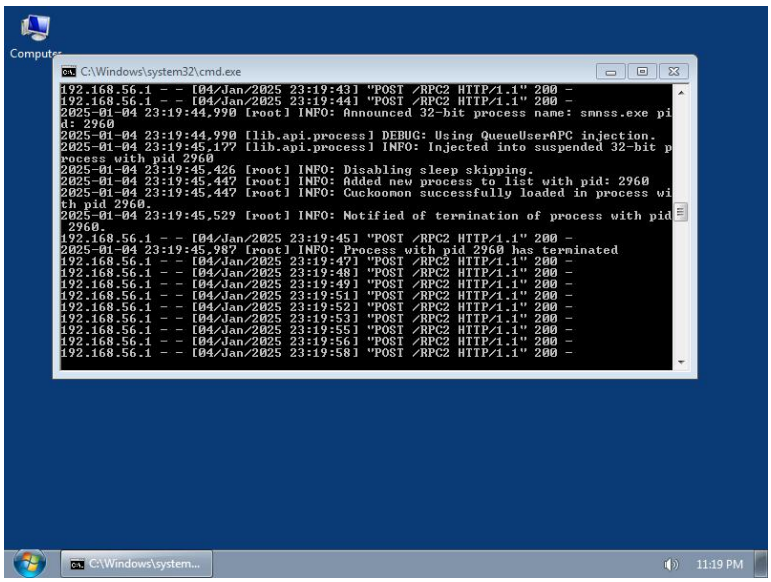

C:\Windows\system32\cmd.exe
d: 3016
2025-01-04 23:22:26,776 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:26,891 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3016
2025-01-04 23:22:26,911 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:26,930 [root] INFO: Added new process to list with pid: 3016
2025-01-04 23:22:26,930 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3016.
2025-01-04 23:22:26,930 [root] INFO: Notified of termination of process with pid
3016.
2025-01-04 23:22:27,332 [root] INFO: Process with pid 3016 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:35] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:36,421 [root] INFO: Analysis timeout hit, terminating analysis.
2025-01-04 23:22:36,421 [root] INFO: Created shutdown mutex.
192.168.56.1 - - [04/Jan/2025 23:22:36] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:37,773 [root] INFO: Shutting down package.
2025-01-04 23:22:37,773 [root] INFO: Stopping auxiliary modules.
C:\Windows\system...
11:22 PM

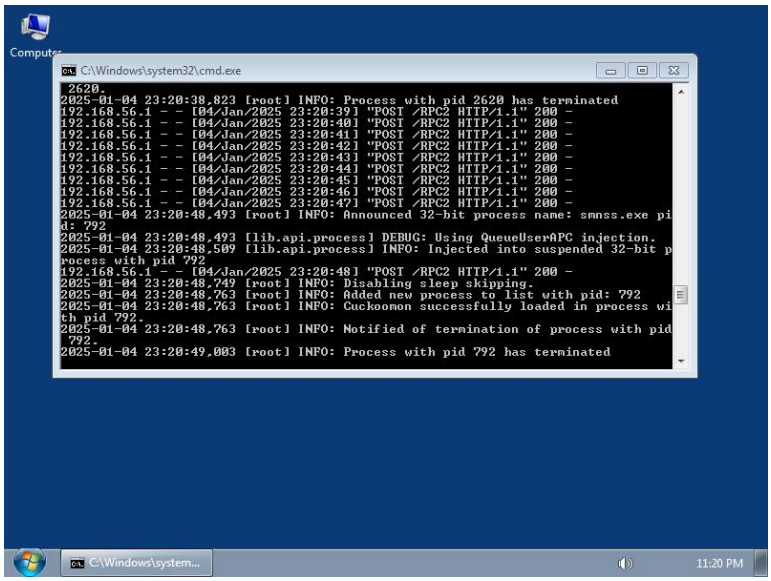

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:57] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:57,938 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2612
2025-01-04 23:20:57,938 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:58,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2612
2025-01-04 23:20:58,601 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [04/Jan/2025 23:20:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:58,844 [root] INFO: Added new process to list with pid: 2612
2025-01-04 23:20:58,844 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2612.
2025-01-04 23:20:58,871 [root] INFO: Notified of termination of process with pid
2612.
2025-01-04 23:20:59,032 [root] INFO: Process with pid 2612 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:00] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

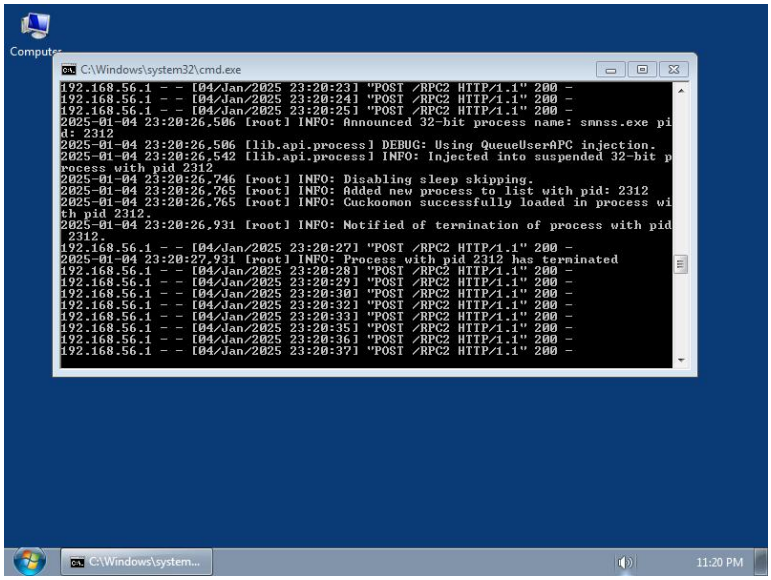

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:44] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:44,990 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2960
2025-01-04 23:19:44,990 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:45,177 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2960
2025-01-04 23:19:45,426 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:45,447 [root] INFO: Added new process to list with pid: 2960
2025-01-04 23:19:45,447 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2960.
2025-01-04 23:19:45,529 [root] INFO: Notified of termination of process with pid
2960.
192.168.56.1 - - [04/Jan/2025 23:19:45] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:45,987 [root] INFO: Process with pid 2960 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:56] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

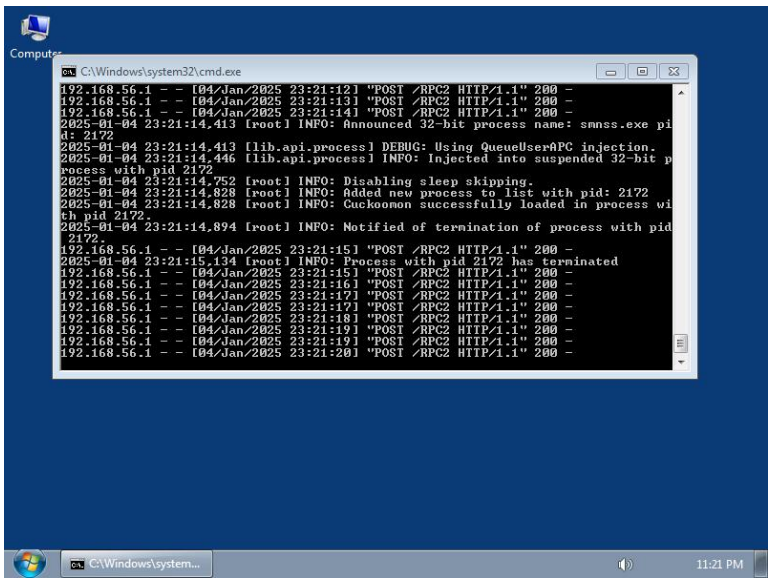

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:06,644 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3020
2025-01-04 23:21:06,657 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:06,681 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3020
2025-01-04 23:21:06,706 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:06,730 [root] INFO: Added new process to list with pid: 3020
2025-01-04 23:21:06,730 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3020.
2025-01-04 23:21:06,875 [root] INFO: Notified of termination of process with pid
 3020.
192.168.56.1 - - [04/Jan/2025 23:21:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:07,203 [root] INFO: Process with pid 3020 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:08] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

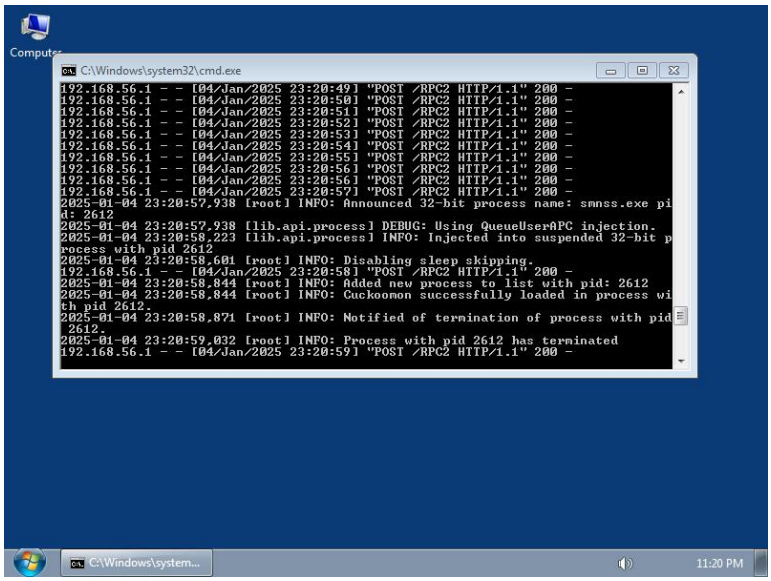

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:27,625 [modules.auxiliary.human] INFO: Found button "Close the
program", clicking it
192.168.56.1 - - [04/Jan/2025 23:19:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:29] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:29,177 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2760
2025-01-04 23:19:29,233 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:29,516 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2760
2025-01-04 23:19:29,573 [root] INFO: Notified of termination of process with pid
 2536.
2025-01-04 23:19:29,838 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:29,933 [root] INFO: Added new process to list with pid: 2760
2025-01-04 23:19:29,933 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2760.
2025-01-04 23:19:30,424 [root] INFO: Process with pid 2536 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:30] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

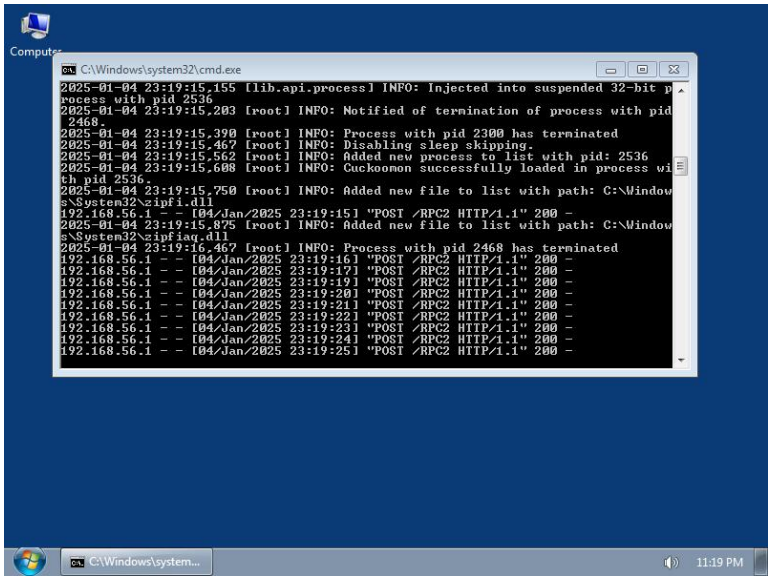

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:44] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:44,990 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2960
2025-01-04 23:19:44,990 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:45,177 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2960
2025-01-04 23:19:45,426 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:45,447 [root] INFO: Added new process to list with pid: 2960
2025-01-04 23:19:45,447 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2960.
2025-01-04 23:19:45,529 [root] INFO: Notified of termination of process with pid
 2960.
192.168.56.1 - - [04/Jan/2025 23:19:45] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:45,987 [root] INFO: Process with pid 2960 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:58] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

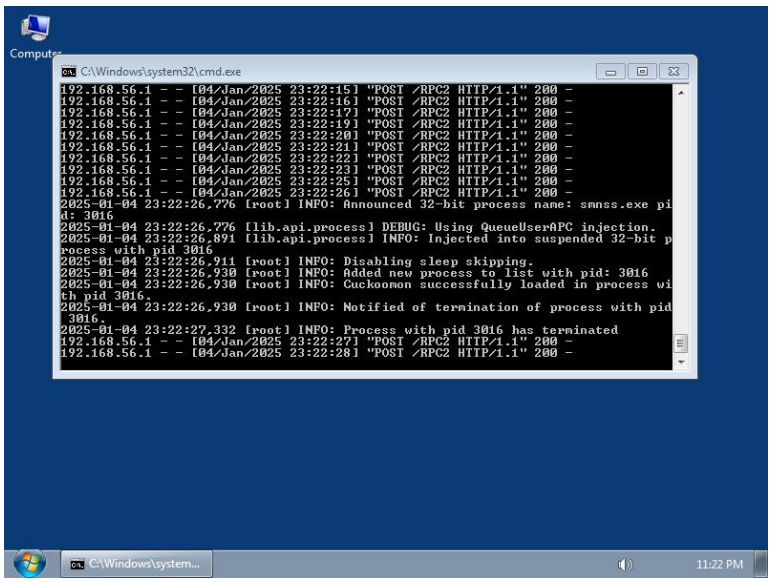

C:\Windows\system32\cmd.exe
2620.
2025-01-04 23:20:38,823 [root] INFO: Process with pid 2620 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:47] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,493 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 792
2025-01-04 23:20:48,493 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:48,509 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 792
192.168.56.1 - - [04/Jan/2025 23:20:48] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,749 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:48,763 [root] INFO: Added new process to list with pid: 792
2025-01-04 23:20:48,763 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 792.
2025-01-04 23:20:48,763 [root] INFO: Notified of termination of process with pid
792.
2025-01-04 23:20:49,003 [root] INFO: Process with pid 792 has terminated
C:\Windows\system...
11:20 PM

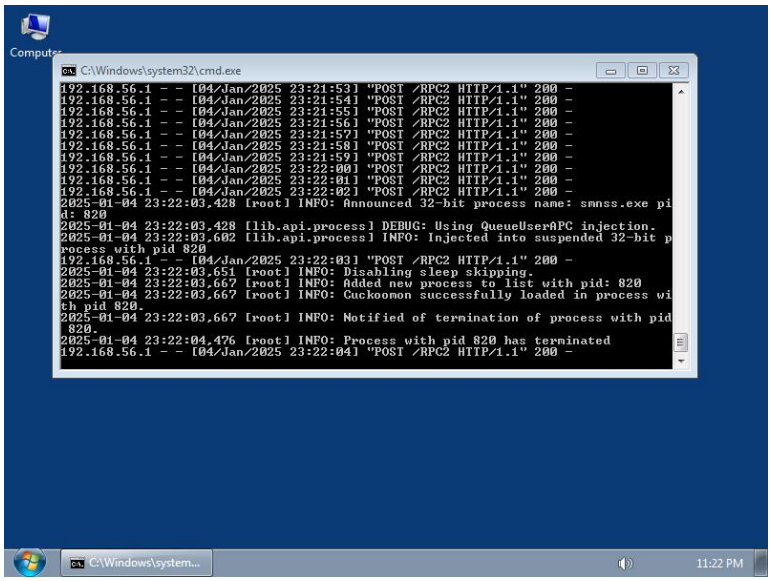

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:25] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:26,506 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2312
2025-01-04 23:20:26,506 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:26,542 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2312
2025-01-04 23:20:26,746 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:26,765 [root] INFO: Added new process to list with pid: 2312
2025-01-04 23:20:26,765 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2312.
2025-01-04 23:20:26,931 [root] INFO: Notified of termination of process with pid
2312.
192.168.56.1 - - [04/Jan/2025 23:20:27] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:27,931 [root] INFO: Process with pid 2312 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:37] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

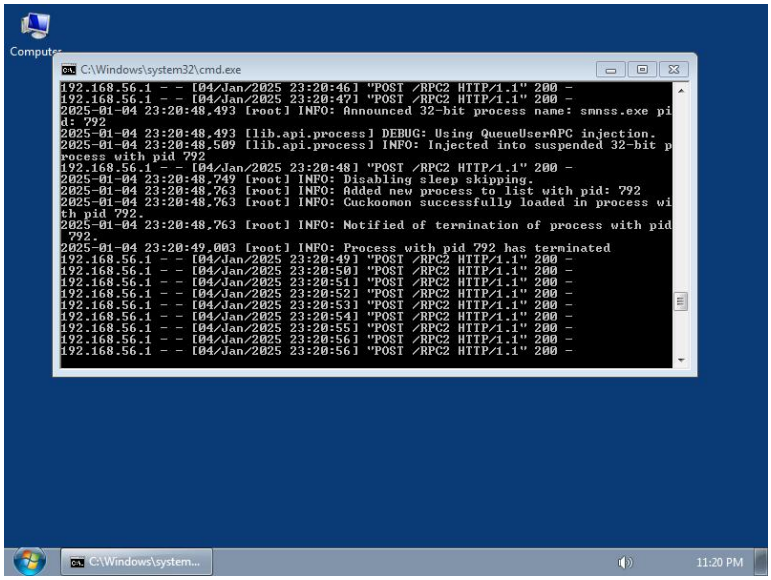

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:14,413 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2172
2025-01-04 23:21:14,413 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:14,446 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2172
2025-01-04 23:21:14,752 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:14,828 [root] INFO: Added new process to list with pid: 2172
2025-01-04 23:21:14,828 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2172.
2025-01-04 23:21:14,894 [root] INFO: Notified of termination of process with pid
2172.
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:15,134 [root] INFO: Process with pid 2172 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:20] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

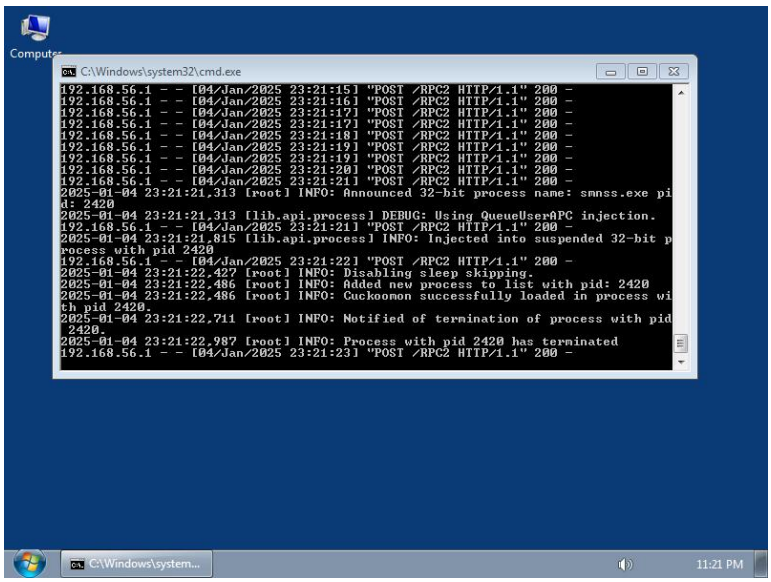

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:57] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:57,938 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2612
2025-01-04 23:20:57,938 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:58,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2612
2025-01-04 23:20:58,601 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [04/Jan/2025 23:20:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:58,844 [root] INFO: Added new process to list with pid: 2612
2025-01-04 23:20:58,844 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2612.
2025-01-04 23:20:58,871 [root] INFO: Notified of termination of process with pid
2612.
2025-01-04 23:20:59,032 [root] INFO: Process with pid 2612 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:59] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

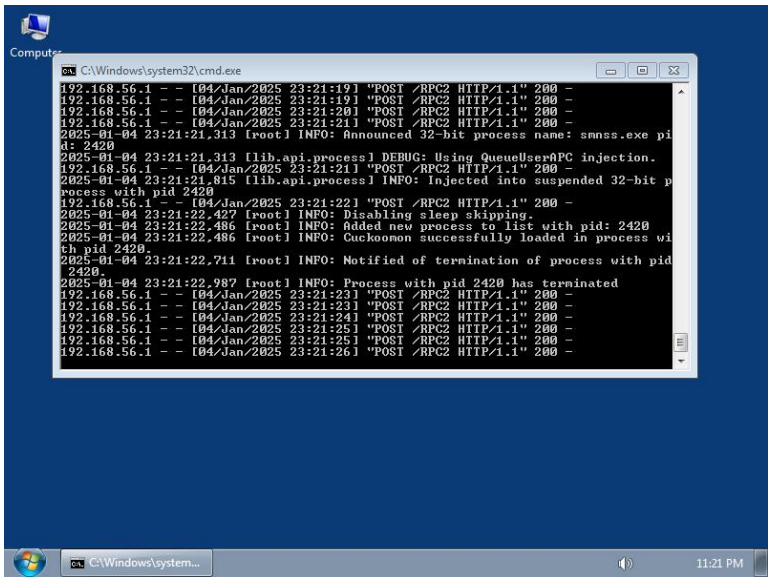

C:\Windows\system32\cmd.exe
2025-01-04 23:19:15,155 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2536
2025-01-04 23:19:15,203 [root] INFO: Notified of termination of process with pid
2468.
2025-01-04 23:19:15,390 [root] INFO: Process with pid 2300 has terminated
2025-01-04 23:19:15,467 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:15,562 [root] INFO: Added new process to list with pid: 2536
2025-01-04 23:19:15,608 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2536.
2025-01-04 23:19:15,750 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfi.dll
192.168.56.1 - - [04/Jan/2025 23:19:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:15,875 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfiaq.dll
2025-01-04 23:19:16,467 [root] INFO: Process with pid 2468 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:25] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM

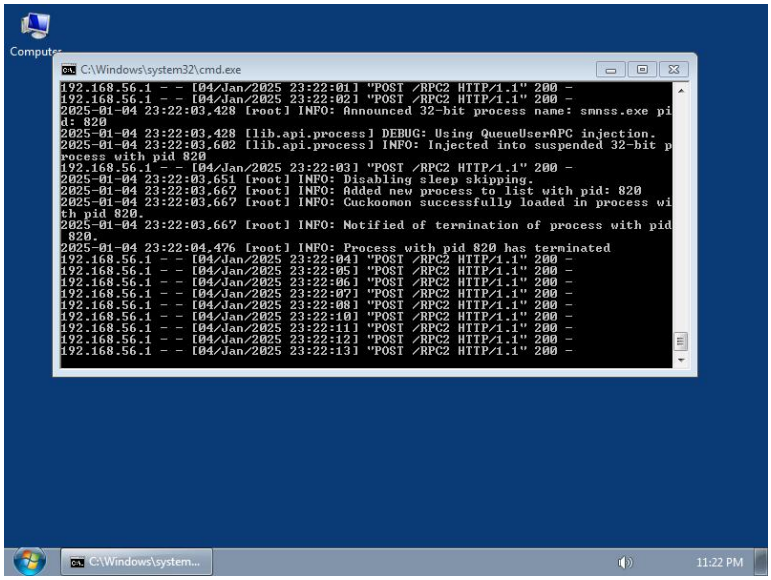

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:26] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:26,776 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 3016
2025-01-04 23:22:26,776 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:26,891 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3016
2025-01-04 23:22:26,911 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:26,930 [root] INFO: Added new process to list with pid: 3016
2025-01-04 23:22:26,930 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3016.
2025-01-04 23:22:26,930 [root] INFO: Notified of termination of process with pid
3016.
2025-01-04 23:22:27,332 [root] INFO: Process with pid 3016 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:28] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

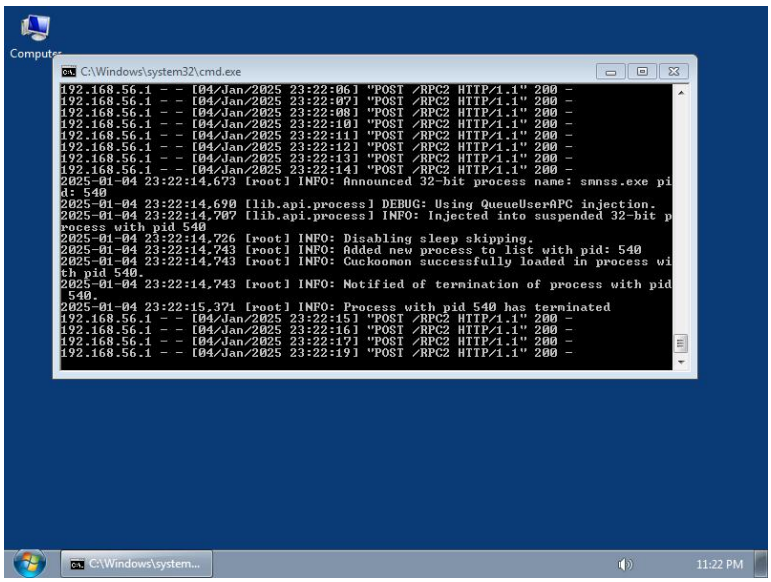

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:02] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,428 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 820
2025-01-04 23:22:03,428 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:03,602 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 820
192.168.56.1 - - [04/Jan/2025 23:22:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,651 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:03,667 [root] INFO: Added new process to list with pid: 820
2025-01-04 23:22:03,667 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 820.
2025-01-04 23:22:03,667 [root] INFO: Notified of termination of process with pid
820.
2025-01-04 23:22:04,476 [root] INFO: Process with pid 820 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:04] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

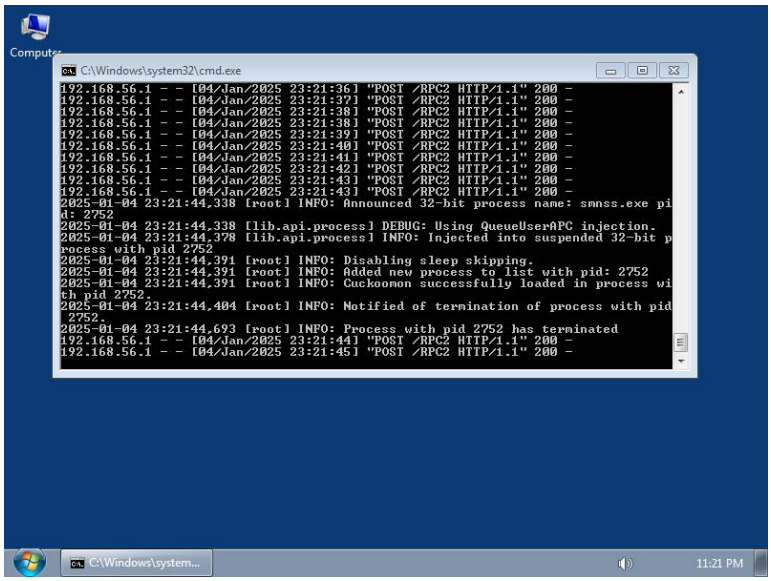

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:47] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,493 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 792
2025-01-04 23:20:48,493 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:48,509 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 792
192.168.56.1 - - [04/Jan/2025 23:20:48] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:48,749 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:48,763 [root] INFO: Added new process to list with pid: 792
2025-01-04 23:20:48,763 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 792.
2025-01-04 23:20:48,763 [root] INFO: Notified of termination of process with pid
792.
2025-01-04 23:20:49,003 [root] INFO: Process with pid 792 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

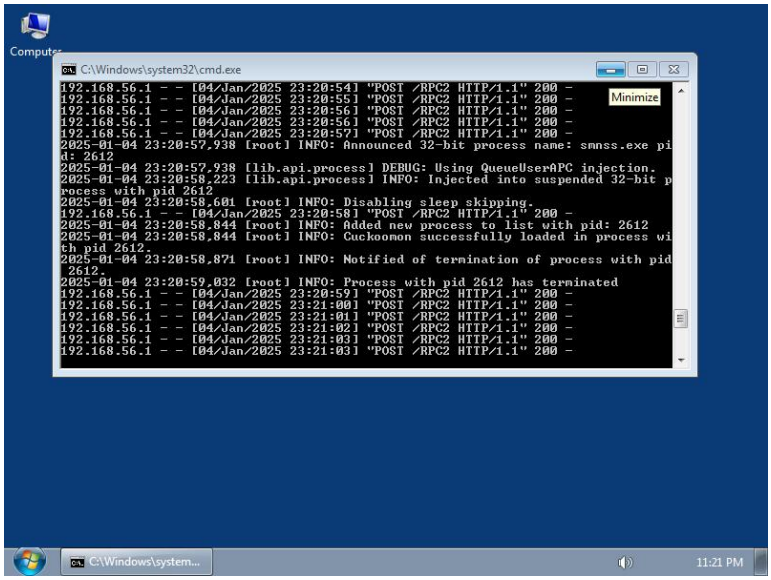

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,313 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2420
2025-01-04 23:21:21,313 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,815 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2420
192.168.56.1 - - [04/Jan/2025 23:21:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:22,427 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:22,486 [root] INFO: Added new process to list with pid: 2420
2025-01-04 23:21:22,486 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2420.
2025-01-04 23:21:22,711 [root] INFO: Notified of termination of process with pid
2420.
2025-01-04 23:21:22,987 [root] INFO: Process with pid 2420 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

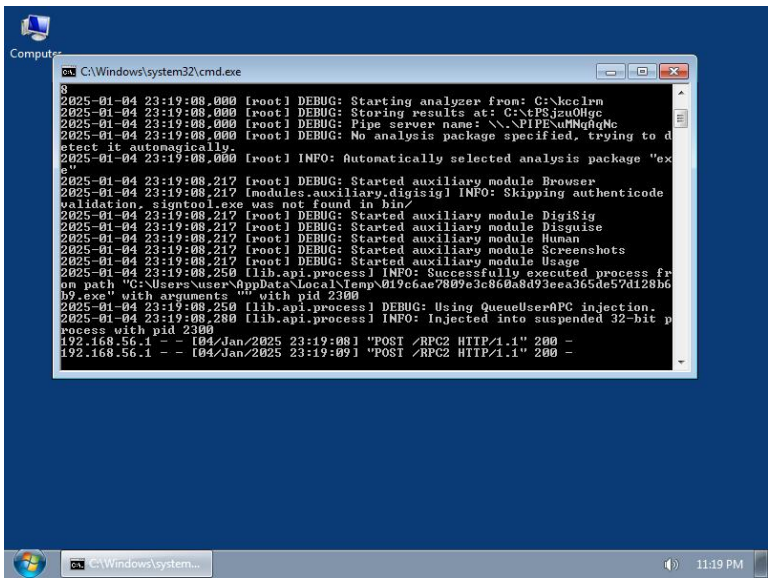

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,313 [root] INFO: Announced 32-bit process name: smnss.exe pid: 2420
2025-01-04 23:21:21,313 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,815 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2420
192.168.56.1 - - [04/Jan/2025 23:21:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:22,427 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:22,486 [root] INFO: Added new process to list with pid: 2420
2025-01-04 23:21:22,486 [root] INFO: Cuckoomon successfully loaded in process with pid 2420.
2025-01-04 23:21:22,711 [root] INFO: Notified of termination of process with pid 2420.
2025-01-04 23:21:22,987 [root] INFO: Process with pid 2420 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:26] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM

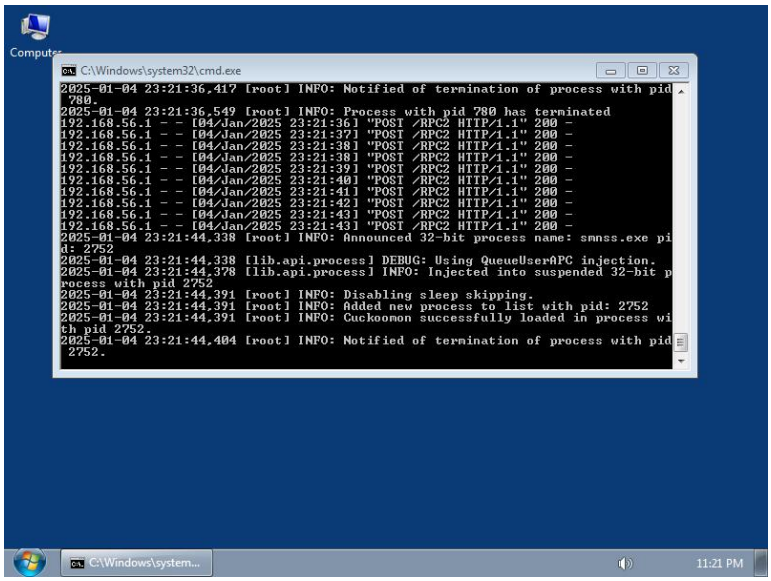

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:02] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,428 [root] INFO: Announced 32-bit process name: smnss.exe pid: 820
2025-01-04 23:22:03,428 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:03,602 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 820
192.168.56.1 - - [04/Jan/2025 23:22:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,651 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:03,667 [root] INFO: Added new process to list with pid: 820
2025-01-04 23:22:03,667 [root] INFO: Cuckoomon successfully loaded in process with pid 820.
2025-01-04 23:22:03,667 [root] INFO: Notified of termination of process with pid 820.
2025-01-04 23:22:04,476 [root] INFO: Process with pid 820 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:13] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

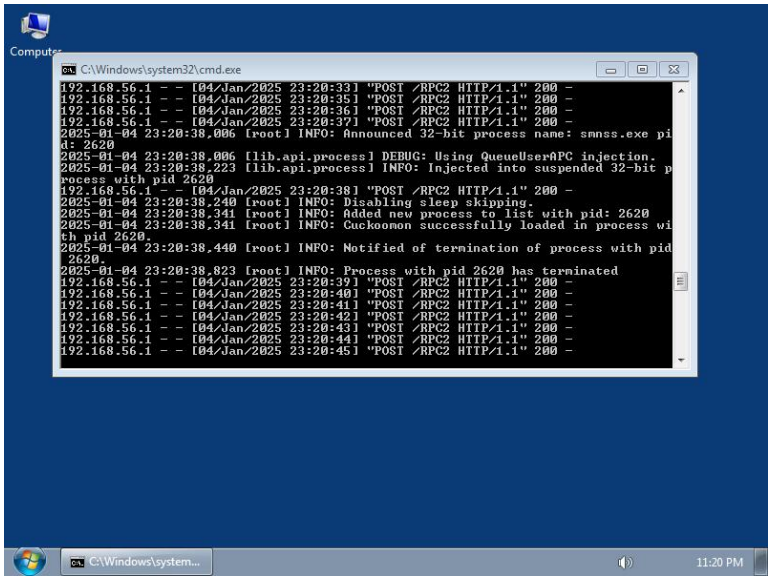

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:22:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:14,673 [root] INFO: Announced 32-bit process name: smnss.exe pid: 540
2025-01-04 23:22:14,690 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:14,707 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 540
2025-01-04 23:22:14,726 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:14,743 [root] INFO: Added new process to list with pid: 540
2025-01-04 23:22:14,743 [root] INFO: Cuckoomon successfully loaded in process with pid 540.
2025-01-04 23:22:14,743 [root] INFO: Notified of termination of process with pid 540.
2025-01-04 23:22:15,371 [root] INFO: Process with pid 540 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:19] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM

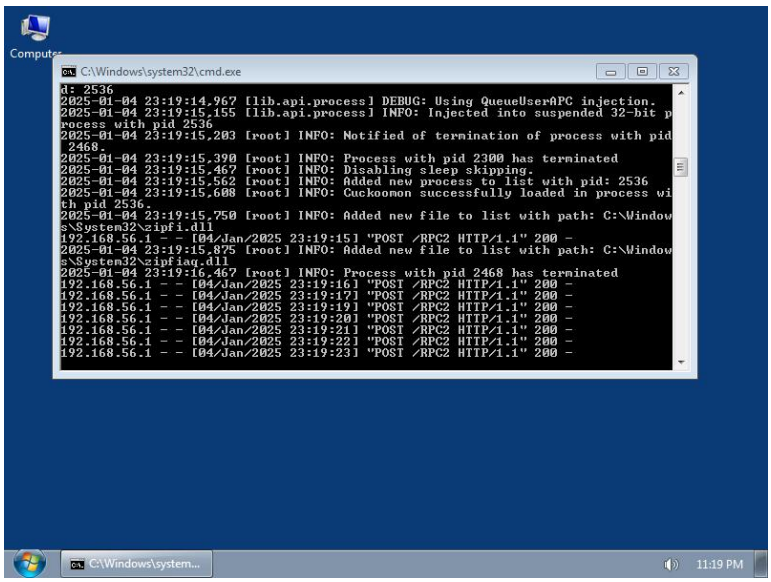

C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:44,338 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2752
2025-01-04 23:21:44,338 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:44,378 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2752
2025-01-04 23:21:44,391 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:44,391 [root] INFO: Added new process to list with pid: 2752
2025-01-04 23:21:44,391 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2752.
2025-01-04 23:21:44,404 [root] INFO: Notified of termination of process with pid
 2752.
2025-01-04 23:21:44,693 [root] INFO: Process with pid 2752 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:45] "POST /RPC2 HTTP/1.1" 200 -
11:21 PM

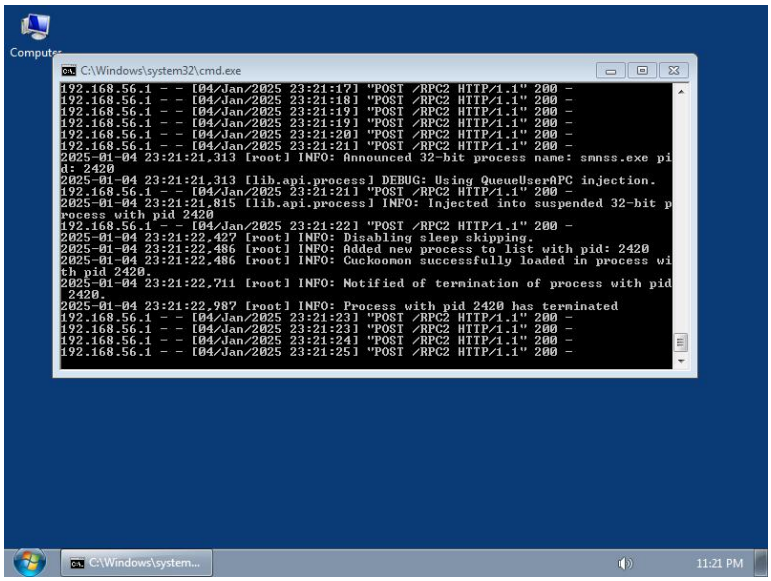

C:\Windows\system32\cmd.exe
Minimize
192.168.56.1 - - [04/Jan/2025 23:20:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:57] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:57,938 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2612
2025-01-04 23:20:57,938 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:58,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2612
2025-01-04 23:20:58,601 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [04/Jan/2025 23:20:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:58,844 [root] INFO: Added new process to list with pid: 2612
2025-01-04 23:20:58,844 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2612.
2025-01-04 23:20:58,871 [root] INFO: Notified of termination of process with pid
 2612.
2025-01-04 23:20:59,032 [root] INFO: Process with pid 2612 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:03] "POST /RPC2 HTTP/1.1" 200 -
11:21 PM

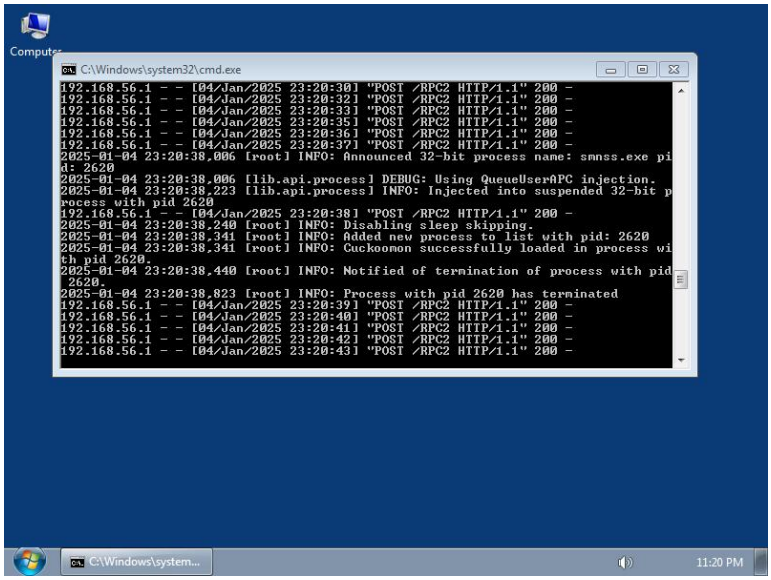

C:\Windows\system32\cmd.exe
8
2025-01-04 23:19:08,000 [root] DEBUG: Starting analyzer from: C:\kcclrm
2025-01-04 23:19:08,000 [root] DEBUG: Storing results at: C:\tPSjzuOHgc
2025-01-04 23:19:08,000 [root] DEBUG: Pipe server name: \\.\PIPE\uMNqRqMc
2025-01-04 23:19:08,000 [root] DEBUG: No analysis package specified, trying to d
etect it automagically.
2025-01-04 23:19:08,000 [root] INFO: Automatically selected analysis package "ex
e"
2025-01-04 23:19:08,217 [root] DEBUG: Started auxiliary module Browser
2025-01-04 23:19:08,217 [modules.auxiliary.digisig] INFO: Skipping authenticode
validation, signtool.exe was not found in bin/
2025-01-04 23:19:08,217 [root] DEBUG: Started auxiliary module DigiSig
2025-01-04 23:19:08,217 [root] DEBUG: Started auxiliary module Disguise
2025-01-04 23:19:08,217 [root] DEBUG: Started auxiliary module Human
2025-01-04 23:19:08,217 [root] DEBUG: Started auxiliary module Screenshots
2025-01-04 23:19:08,217 [root] DEBUG: Started auxiliary module Usage
2025-01-04 23:19:08,250 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\019c6ae7809e3c860a8d93eea365de57d128b6
b9.exe" with arguments "" with pid 2300
2025-01-04 23:19:08,250 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:08,280 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2300
192.168.56.1 - - [04/Jan/2025 23:19:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:09] "POST /RPC2 HTTP/1.1" 200 -
11:19 PM

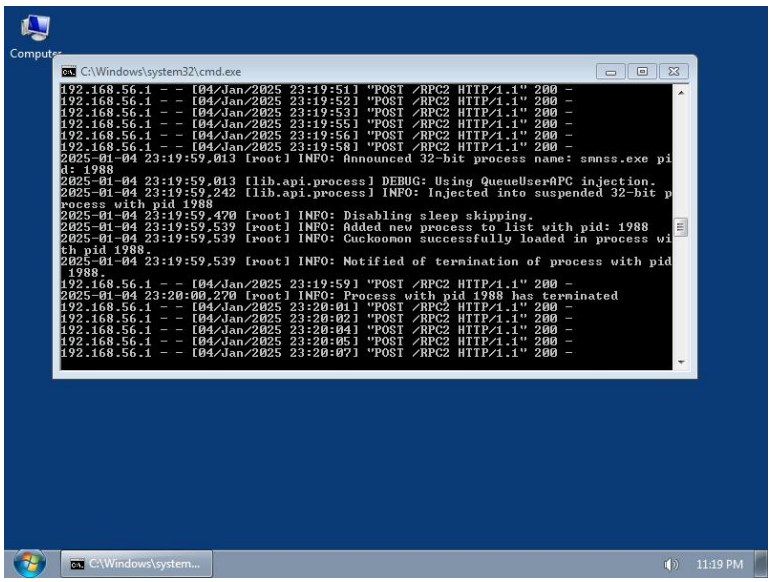

Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:21:36,417 [root] INFO: Notified of termination of process with pid
780.
2025-01-04 23:21:36,549 [root] INFO: Process with pid 780 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:43] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:44,338 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2752
2025-01-04 23:21:44,338 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:21:44,378 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2752
2025-01-04 23:21:44,391 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:44,391 [root] INFO: Added new process to list with pid: 2752
2025-01-04 23:21:44,391 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2752.
2025-01-04 23:21:44,404 [root] INFO: Notified of termination of process with pid
2752.
C:\Windows\system...
11:21 PM

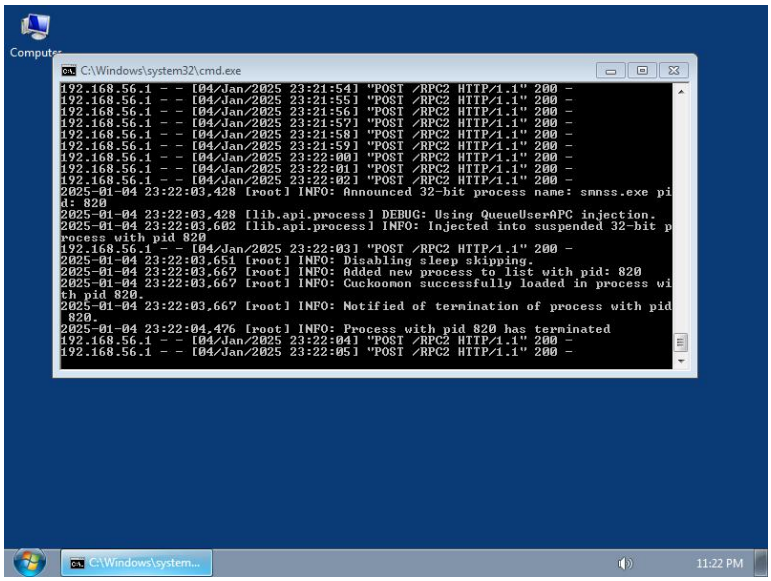

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:37] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,006 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2620
2025-01-04 23:20:38,006 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:38,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2620
192.168.56.1 - - [04/Jan/2025 23:20:38] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,240 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:38,341 [root] INFO: Added new process to list with pid: 2620
2025-01-04 23:20:38,341 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2620.
2025-01-04 23:20:38,440 [root] INFO: Notified of termination of process with pid
2620.
2025-01-04 23:20:38,823 [root] INFO: Process with pid 2620 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:45] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM

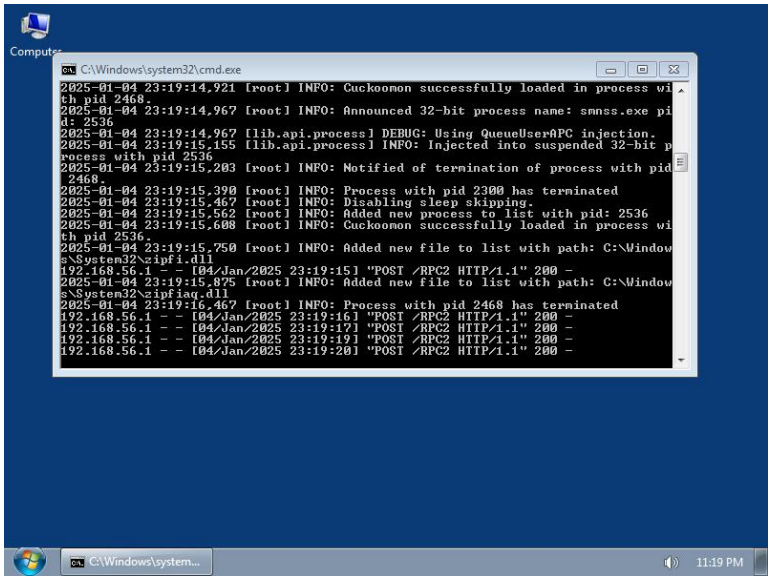

Computer
C:\Windows\system32\cmd.exe
d: 2536
2025-01-04 23:19:14,967 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:15,155 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2536
2025-01-04 23:19:15,203 [root] INFO: Notified of termination of process with pid
2468.
2025-01-04 23:19:15,390 [root] INFO: Process with pid 2300 has terminated
2025-01-04 23:19:15,467 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:15,562 [root] INFO: Added new process to list with pid: 2536
2025-01-04 23:19:15,608 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2536.
2025-01-04 23:19:15,750 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfi.dll
192.168.56.1 - - [04/Jan/2025 23:19:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:15,875 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfiaq.dll
2025-01-04 23:19:16,467 [root] INFO: Process with pid 2468 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:23] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM


Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,313 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2420
2025-01-04 23:21:21,313 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [04/Jan/2025 23:21:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:21,815 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2420
192.168.56.1 - - [04/Jan/2025 23:21:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:21:22,427 [root] INFO: Disabling sleep skipping.
2025-01-04 23:21:22,486 [root] INFO: Added new process to list with pid: 2420
2025-01-04 23:21:22,486 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2420.
2025-01-04 23:21:22,711 [root] INFO: Notified of termination of process with pid
 2420.
2025-01-04 23:21:22,987 [root] INFO: Process with pid 2420 has terminated
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:25] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:21 PM


Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:20:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:37] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,006 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2620
2025-01-04 23:20:38,006 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:20:38,223 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2620
192.168.56.1 - - [04/Jan/2025 23:20:38] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:38,240 [root] INFO: Disabling sleep skipping.
2025-01-04 23:20:38,341 [root] INFO: Added new process to list with pid: 2620
2025-01-04 23:20:38,341 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2620.
2025-01-04 23:20:38,440 [root] INFO: Notified of termination of process with pid
 2620.
2025-01-04 23:20:38,823 [root] INFO: Process with pid 2620 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:43] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:20 PM


Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:19:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:59,013 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 1988
2025-01-04 23:19:59,013 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:59,242 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 1988
2025-01-04 23:19:59,470 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:59,539 [root] INFO: Added new process to list with pid: 1988
2025-01-04 23:19:59,539 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 1988.
2025-01-04 23:19:59,539 [root] INFO: Notified of termination of process with pid
 1988.
192.168.56.1 - - [04/Jan/2025 23:19:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:20:00,270 [root] INFO: Process with pid 1988 has terminated
192.168.56.1 - - [04/Jan/2025 23:20:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:20:07] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM


Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [04/Jan/2025 23:21:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:21:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:02] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,428 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 820
2025-01-04 23:22:03,428 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:22:03,602 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 820
192.168.56.1 - - [04/Jan/2025 23:22:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:22:03,651 [root] INFO: Disabling sleep skipping.
2025-01-04 23:22:03,667 [root] INFO: Added new process to list with pid: 820
2025-01-04 23:22:03,667 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 820.
2025-01-04 23:22:03,667 [root] INFO: Notified of termination of process with pid
 820.
2025-01-04 23:22:04,476 [root] INFO: Process with pid 820 has terminated
192.168.56.1 - - [04/Jan/2025 23:22:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:22:05] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:22 PM


Computer
C:\Windows\system32\cmd.exe
2025-01-04 23:19:14,921 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2468.
2025-01-04 23:19:14,967 [root] INFO: Announced 32-bit process name: smnss.exe pi
d: 2536
2025-01-04 23:19:14,967 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-04 23:19:15,155 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2536
2025-01-04 23:19:15,203 [root] INFO: Notified of termination of process with pid
 2468.
2025-01-04 23:19:15,390 [root] INFO: Process with pid 2300 has terminated
2025-01-04 23:19:15,467 [root] INFO: Disabling sleep skipping.
2025-01-04 23:19:15,562 [root] INFO: Added new process to list with pid: 2536
2025-01-04 23:19:15,608 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2536.
2025-01-04 23:19:15,750 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfi.dll
192.168.56.1 - - [04/Jan/2025 23:19:15] "POST /RPC2 HTTP/1.1" 200 -
2025-01-04 23:19:15,875 [root] INFO: Added new file to list with path: C:\Window
s\System32\zipfiaq.dll
2025-01-04 23:19:16,467 [root] INFO: Process with pid 2468 has terminated
192.168.56.1 - - [04/Jan/2025 23:19:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [04/Jan/2025 23:19:20] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
11:19 PM