

Summary

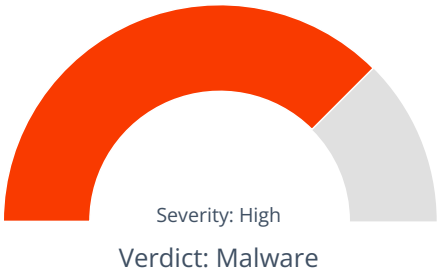
File Name: 198808e07a5ff1f81792f5d8ad348117d57331ee
File Type: PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
SHA1: 198808e07a5ff1f81792f5d8ad348117d57331ee
MD5: 8e8b92bdefe259ace73cf93e3313330b



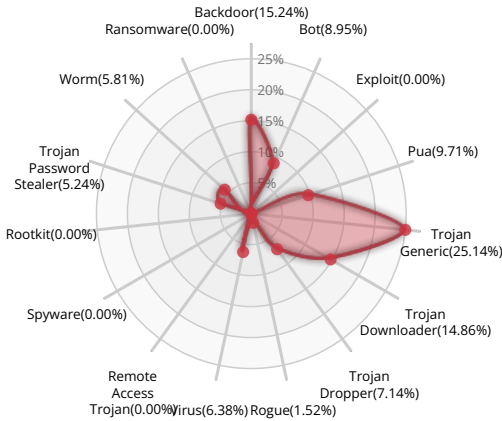
MALWARE

Valkyrie Final Verdict

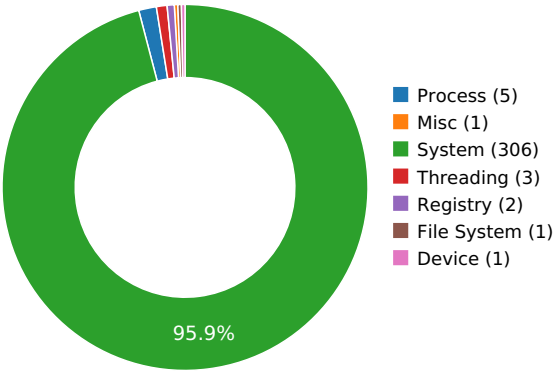
DETECTION SECTION



CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



Activity Details

MALWARE ANALYSIS SYSTEM EVASION



Possible date expiration check, exits too soon after checking local time

Show sources

Network activity detected but not expressed in API logs

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION



Creates RWX memory

Show sources

Behavior Graph

10:32:4910:33:2310:33:56

PID 2460

10:32:49

Create Process

The malicious file created a child process as 198808e07a5ff1f81792f5d8ad348117d57331ee.exe (PPID 2396)

10:33:55

Create Process

10:33:56

NtAllocateVirtualMem

10:33:56

NtTerminateProcess

Behavior Summary

RESOLVED APIS

kernel32.dll.AddVectoredContinueHandler

kernel32.dll.GetQueuedCompletionStatusEx

kernel32.dll.LoadLibraryExA

kernel32.dll.LoadLibraryExW

advapi32.dll.SystemFunction036

ntdll.dll.NtWaitForSingleObject

winmm.dll.timeBeginPeriod

winmm.dll.timeEndPeriod

ws2_32.dll.WSAGetOverlappedResult

cryptbase.dll.SystemFunction001

cryptbase.dll.SystemFunction002

cryptbase.dll.SystemFunction003

cryptbase.dll.SystemFunction004

cryptbase.dll.SystemFunction005

cryptbase.dll.SystemFunction028

cryptbase.dll.SystemFunction029

cryptbase.dll.SystemFunction034

cryptbase.dll.SystemFunction036

cryptbase.dll.SystemFunction040

cryptbase.dll.SystemFunction041

kernel32.dll.GetStdHandle

kernel32.dll.SetHandleInformation

kernel32.dll.GetSystemDirectoryW

kernel32.dll.CreateFileMappingW

kernel32.dll.MapViewOfFile

kernel32.dll.IsBadReadPtr

kernel32.dll.VirtualAlloc

kernel32.dll.UnmapViewOfFile

kernel32.dll.CloseHandle

kernel32.dll.VirtualFree

kernel32.dll.CreateProcessW

kernel32.dll.VirtualAllocEx

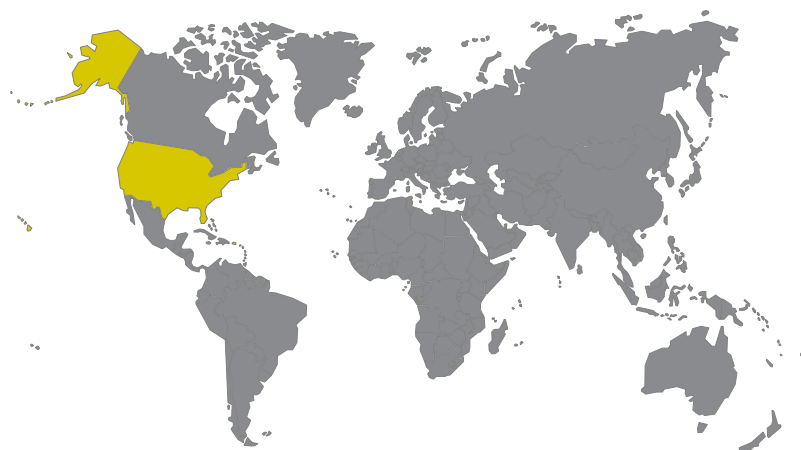
REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize

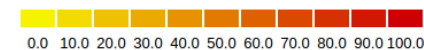
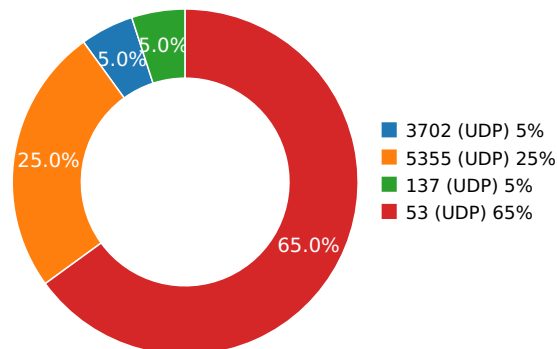
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Google LLC	Malware Process
	8.8.8.8	United States	15169	Google LLC	Malware Process
					Malware Process
www.msftncsi.com	23.200.3.18	United States	20940	Akamai Technologies, Inc.	Malware Process
www.aieov.com	76.223.54.146	United States	16509	Amazon.com, Inc.	Malware Process

DNS QUERIES

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

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.20490694046	Sandbox	224.0.0.252	5355
3.20609712601	Sandbox	224.0.0.252	5355
3.2171959877	Sandbox	239.255.255.250	3702
3.2261941433	Sandbox	224.0.0.252	5355
3.24472093582	Sandbox	192.168.56.255	137
4.5049431324	Sandbox	224.0.0.252	5355
5.93450593948	Sandbox	224.0.0.252	5355
5.96880793571	Sandbox	8.8.4.4	53
6.96949410439	Sandbox	8.8.8.8	53
7.26642298698	Sandbox	8.8.4.4	53
8.27079296112	Sandbox	8.8.8.8	53
21.6813211441	Sandbox	8.8.8.8	53
22.6867649555	Sandbox	8.8.4.4	53
36.2022790909	Sandbox	8.8.8.8	53
37.2107579708	Sandbox	8.8.4.4	53
51.511070013	Sandbox	8.8.8.8	53
52.5206129551	Sandbox	8.8.4.4	53
66.0939369202	Sandbox	8.8.8.8	53
67.1084270477	Sandbox	8.8.4.4	53
80.5577669144	Sandbox	8.8.8.8	53

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
-----------	-----------------

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	198808e07a5ff1f81792f5d8ad348117d57331ee
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
SHA1:	198808e07a5ff1f81792f5d8ad348117d57331ee
MD5:	8e8b92bdefe259ace73cf93e3313330b
First Seen Date:	2025-08-20 07:24:02.865486 (about 3 hours ago)
Number Of Clients Seen:	1
Last Analysis Date:	2025-08-20 07:24:02.865486 (about 3 hours ago)
Human Expert Analysis Date:	2025-08-20 10:23:07.559651 (20 minutes ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	4
File Type Enum	7
Debug Artifacts	[]
Number Of Sections	5
Trid	[[87.2, u'Win64 Executable (generic)'], [6.3, u'Generic Win/DOS Executable'], [6.3, u'DOS Executable Generic'], [0.0, u'VXD Driver']]
Compilation Time Stamp	0x0 [Thu Jan 1 00:00:00 1970 UTC] [SUSPICIOUS]
LegalCopyright	Copyright (c) 2025 UltiMaker
ProductName	UltiMaker Cura 5.10.2
FileDescription	Application
FileVersion	5.10.2.0
CompanyName	UltiMaker
Translation	0x0409 0x04b0
Entry Point	0x450e10 (.text)
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
File Size	1832536
Ssdeep	24576:rm0urnSzpnH2ppdVtnsf85PPszpqmkU6ggjZDkXjxOVy:60UnStnMplImkU6ggFDwv
Sha256	f910c521a834e26b995ccb52d49bc73dd5b0a6450dbc8c416e41af5204d04e1b
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/1/9/8/8/198808e07a5ff1f81792f5d8ad348117d57331ee', u'EXE:ProductName': u'UltiMaker Cura 5.10.2', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2025:08:20 07:22:55+00:00', u'EXE:InitializedDataSize': 1819648, u'File:FileModifyDate': u'2025:08:20 07:22:23+00:00', u'EXE:FileVersionNumber': u'5.10.2.0', u'EXE:FileVersion': u'5.10.2.0', u'File:FileSize': u'1790 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'AMD AMD64', u'EXE:FileOS': u'Win32', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win64 EXE', u'EXE:CompanyName': u'UltiMaker', u'File:FileName': u'198808e07a5ff1f81792f5d8ad348117d57331ee', u'EXE:ImageVersion': 1.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 6.1, u'EXE:PEType': u'PE32+', u'EXE:TimeStamp': u'0000:00:00 00:00:00', u'EXE:FileFlagsMask': u'0x0000', u'EXE:LegalCopyright': u'Copyright (c) 2025 UltiMaker', u'EXE:LinkerVersion': 2.36, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/1/9/8/8', u'EXE:FileDescription': u'Application', u'EXE:EntryPoint': u'0x50e10', u'EXE:SubsystemVersion': 6.1, u'EXE:CodeSize': 533504, u'File:FileInodeChangeDate': u'2025:08:20 07:22:55+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'5.10.2.0'}]
Mime Type	application/x-dosexec
Imphash	25c4fb4a248389347ae9cf0ce6995420

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x83000	0x82400	5.91995706434	3468fb0a04bee1ae0a5d814dc4c9fa0e
.rdata	0x84000	0x12e000	0x12d200	6.38869511425	2fd5ad3e18975edc509214570b2547be
.data	0x1b2000	0x24000	0x3000	2.51933349184	b7033ce715f4cd1240016f5b4bd0b192
.idata	0x1d6000	0x392	0x400	3.96046714582	101763fc99007de06ded6c4f36aecf2f
.rsrc	0x1d7000	0x99b8	0x9a00	5.41648348863	f30e5b3dcb4481b63a520875f6b1ea95

PE Imports

- kernel32.dll
 - WriteFile
 - WriteConsoleW
 - WaitForMultipleObjects
 - WaitForSingleObject
 - VirtualQuery
 - VirtualFree
 - VirtualAlloc
 - SwitchToThread
 - SetWaitableTimer
 - SetUnhandledExceptionFilter
 - SetProcessPriorityBoost
 - SetEvent
 - SetErrorMode
 - SetConsoleCtrlHandler
 - LoadLibraryA
 - LoadLibraryW
 - GetSystemInfo
 - GetSystemDirectoryA
 - GetStdHandle
 - GetQueuedCompletionStatus
 - GetProcessAffinityMask
 - GetProcAddress
 - GetEnvironmentStringsW
 - GetConsoleMode
 - FreeEnvironmentStringsW
 - ExitProcess
 - DuplicateHandle
 - CreateThread
 - CreateEventA
 - CloseHandle
 - AddVectoredExceptionHandler

PE Resources

{'lang': 'u'LANG_NEUTRAL', 'name': 'u'RT_ICON', 'offset': 1930024, 'sha256': u'bcee1b477b7d0bf7978dd51b33bc6ee9ab4113d177fdf2359701ff3e3398a024', 'type': 'u'GLS_BINARY_LSB_FIRST', 'size': 296}

{'lang': 'u'LANG_NEUTRAL', 'name': 'u'RT_ICON', 'offset': 1930320, 'sha256': u'8e868f6b8bea2ac1ef09abc7d811abb3509d65cdcf6593c968ebf23d00a2c410', 'type': 'u'dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0', 'size': 2216}

{'lang': 'u'LANG_NEUTRAL', 'name': 'u'RT_ICON', 'offset': 1932536, 'sha256': u'418ad9c831d76c773dd5ace964cbd0b936f8deb7fa714d1b882eda679d35efe8', 'type': 'u'data', 'size': 3752}

{'lang': 'u'LANG_NEUTRAL', 'name': 'u'RT_ICON', 'offset': 1936288, 'sha256': u'b59f14f86d9840fa6d84390a6f6adb23c7a66e6807735c46a4f6af17f9a2d2db', 'type': 'u'dBase IV DBT, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0', 'size': 19496}

{'lang': 'u'LANG_NEUTRAL', 'name': 'u'RT_ICON', 'offset': 1955784, 'sha256': u'0fadade1a98aab55b17176408794a224fb85470addf900dabf6b443af543f7834', 'type': 'u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', 'size': 9580}

{'lang': 'u'LANG_ENGLISH', 'name': 'u'RT_DIALOG', 'offset': 1965364, 'sha256': u'7854e8d67a11148566ad37c5d23e1534e0990fe31a160e0e7da3ca751830bb50', 'type': 'u'data', 'size': 180}

{'lang': 'u'LANG_ENGLISH', 'name': 'u'RT_DIALOG', 'offset': 1965544, 'sha256': u'c50631fc1f8425a95fd1edcc8e730d339e193a38f18d42372c32847a5ad2c016', 'type': 'u'data', 'size': 288}

{'lang': 'u'LANG_ENGLISH', 'name': 'u'RT_DIALOG', 'offset': 1965832, 'sha256': u'425b8270f7ca42a927eae6bea468acf414a3e4b58b5ba2c56aaae4d1b2c11014', 'type': 'u'data', 'size': 514}

{'lang': 'u'LANG_ENGLISH', 'name': 'u'RT_DIALOG', 'offset': 1966348, 'sha256': u'4a55bd714f5d50cd8eabba10e57f0618f1842717dcfa582d73a917b1933cd1d4', 'type': 'u'data', 'size': 248}

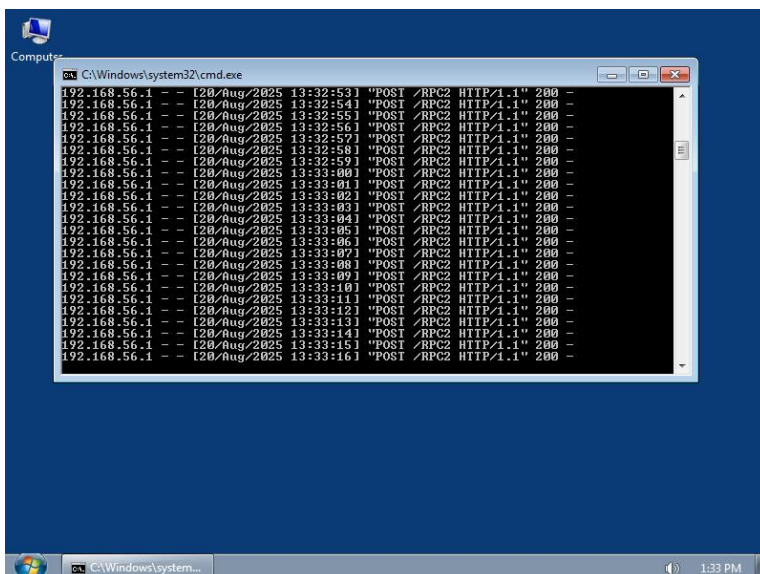
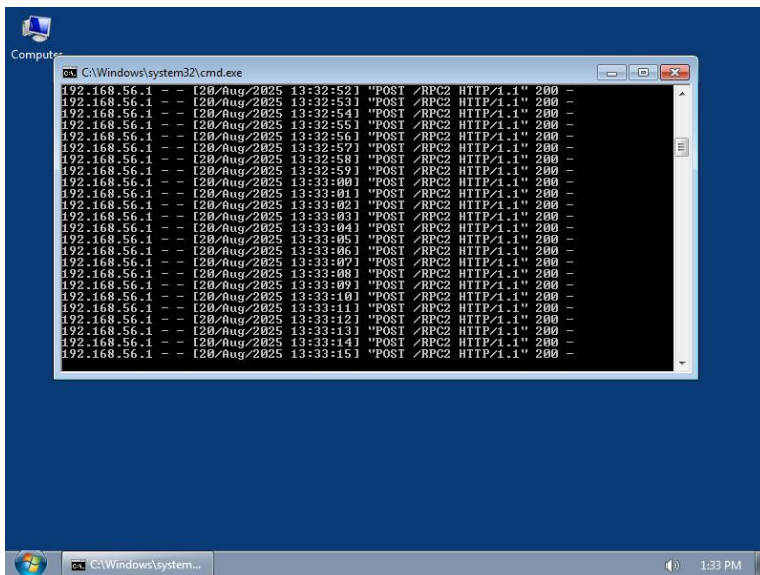
{'lang': 'u'LANG_ENGLISH', 'name': 'u'RT_DIALOG', 'offset': 1966596, 'sha256': u'a7e5ea849cb343e9b58de221aeb25c9dd4a3748070bfa879a30c4265fc39023', 'type': 'u'data', 'size': 160}

```
{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 1966756, u'sha256':
u'587a03198c39f990e77691056bb5705e21374281862ce06de94c68172f50f763', u'type': u'data', u'size': 238}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 1966996, u'sha256':
u'2de709cec9752b6de6b0f3df0c594f280490681962be9000cf813f0d054a090a', u'type': u'MS Windows icon resource - 5 icons, 16x16, 16 colors',
u'size': 76}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 1967072, u'sha256':
u'2f793ae17f1e9c42ee4b7a9c53e5d2ca2c8862d8bc75eeaa80e5a2f6f768e15a', u'type': u'data', u'size': 560}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 1967632, u'sha256':
u'5173bf28b577935c8ec392d8a243a6aae0d4a514d126d6b761fd504f36b38763', u'type': u'XML 1.0 document, ASCII text, with very long lines, with
CRLF line terminators', u'size': 936}
```

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS



```

Computers
C:\Windows\system32\cmd.exe

th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - [20/Aug/2025 13:33:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:55] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:33:56.362 [root] INFO: Notified of termination of process with pid 2460.
2025-08-20 13:33:56.661 [root] INFO: Process with pid 2460 has terminated

```

```

Computers
C:\Windows\system32\cmd.exe

2025-08-20 13:32:39.000 [root] INFO: Date set to: 08-20-25, time set to: 10:32:39
2025-08-20 13:32:39.015 [root] DEBUG: Starting analyzer from: C:\csckvaf1
2025-08-20 13:32:39.015 [root] DEBUG: Storing results at: C:\bF2QEeJbb
2025-08-20 13:32:39.015 [root] DEBUG: Pipe server name: \\.\PIPE\MFNRBqX
2025-08-20 13:32:39.015 [root] DEBUG: No analysis package specified, trying to detect it automatically.
2025-08-20 13:32:39.015 [root] INFO: Automatically selected analysis package "ex"
2025-08-20 13:32:39.203 [root] DEBUG: Started auxiliary module Browser
2025-08-20 13:32:39.203 [modules.auxiliary.digisig] INFO: Skipping authenticode validation, signtool.exe was not found in bin/
2025-08-20 13:32:39.203 [root] DEBUG: Started auxiliary module Digisig
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Disguise
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Human
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Screenshots
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Usage
2025-08-20 13:32:39.280 [lib.api.process] INFO: Successfully executed process from path "C:\Users\User\AppData\Local\Temp\198808e07a5ff1f81792f5d8ad348117d57331ee.exe" with arguments "" with pid 2460
2025-08-20 13:32:39.280 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2460
192.168.56.1 - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

2025-08-20 13:32:39.203 [modules.auxiliary.digisig] INFO: Skipping authenticode
validation, signtool.exe was not found in bin/
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module DigiSig
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Disguise
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Human
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Screenshots
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Usage
2025-08-20 13:32:39.280 [lib.api.process] INFO: Successfully executed process fr
on path "C:\Users\User\AppData\Local\Temp\198808e07a5ff1f81792f5d8ad348117d57331
ee.exe" with arguments "" with pid 2460
2025-08-20 13:32:39.280 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2460
192.168.56.1 - - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckoonon successfully loaded in process wi
th pid 2460
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Human
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Screenshots
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Usage
2025-08-20 13:32:39.280 [lib.api.process] INFO: Successfully executed process fr
on path "C:\Users\User\AppData\Local\Temp\198808e07a5ff1f81792f5d8ad348117d57331
ee.exe" with arguments "" with pid 2460
2025-08-20 13:32:39.280 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2460
192.168.56.1 - - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckoonon successfully loaded in process wi
th pid 2460
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:37] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Disguise
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Human
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Screenshots
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Usage
2025-08-20 13:32:39.200 [lib.api.process] INFO: Successfully executed process fi
on path "C:\Users\User\AppData\Local\Temp\198808e07a5ff1f81792f5d8ad348117d57331
ee.exe" with arguments "" with pid 2460
2025-08-20 13:32:39.312 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2460
192.168.56.1 - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckooon successfully loaded in process wi
th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.927 [root] INFO: Disabling sleep skipping.
192.168.56.1 - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:29] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

validation, signtool.exe was not found in bin/
2025-08-20 13:32:39.203 [root] DEBUG: Started auxiliary module DigiSig
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Disguise
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Human
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Screenshots
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Usage
2025-08-20 13:32:39.200 [lib.api.process] INFO: Successfully executed process fr
on path "C:\Users\User\AppData\Local\Temp\198808e07a5ff1f81792f5d8ad348117d57331
ee.exe" with arguments with pid 2460
2025-08-20 13:32:39.312 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2460
192.168.56.1 - - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckooon successfully loaded in process wi
th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - - [20/Aug/2025 13:33:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:45] "POST /RPC2 HTTP/1.1" 200 -

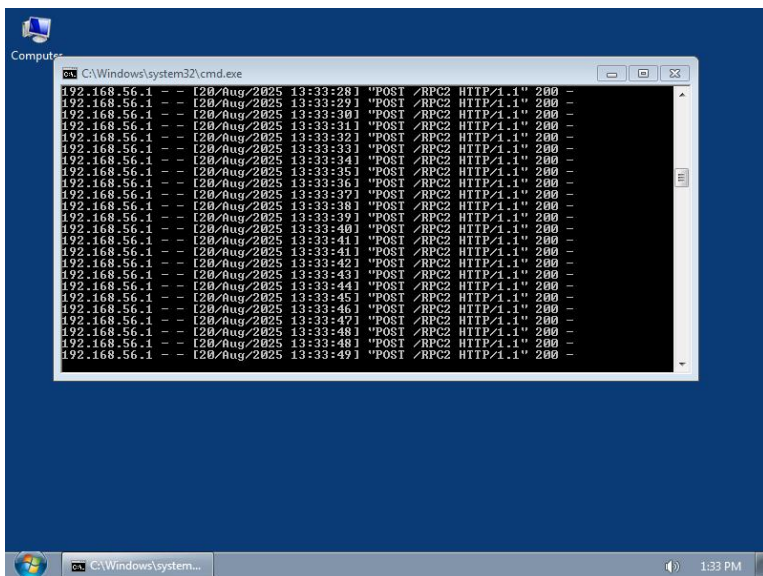
```

```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:42] "POST /RPC2 HTTP/1.1" 200 -

```



```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:34] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Usage
2025-08-20 13:32:39.280 [lib.api.process] INFO: Successfully executed process fr
on path "C:\Users\User\AppData\Local\Temp\198808e07a5ff1f81792f5d8ad348117d57331
ee.exe" with arguments "" with pid 2460
2025-08-20 13:32:39.280 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2460
192.168.56.1 - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckoonon successfully loaded in process wi
th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -

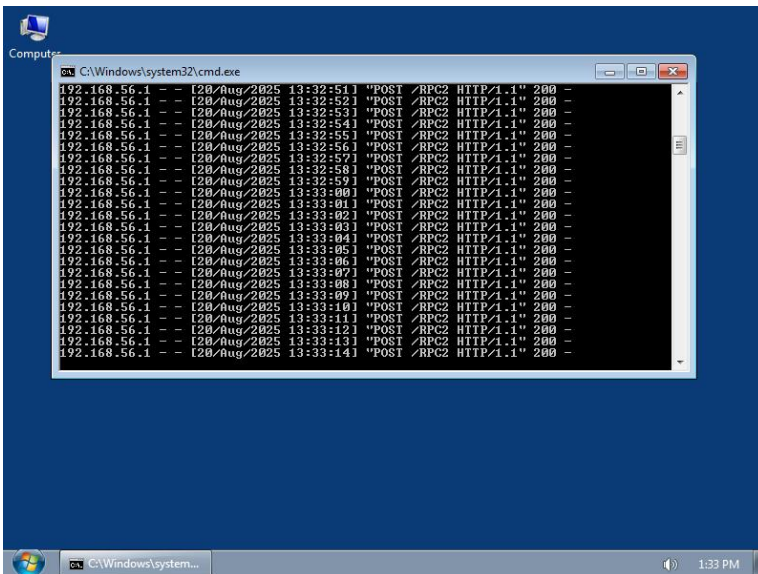
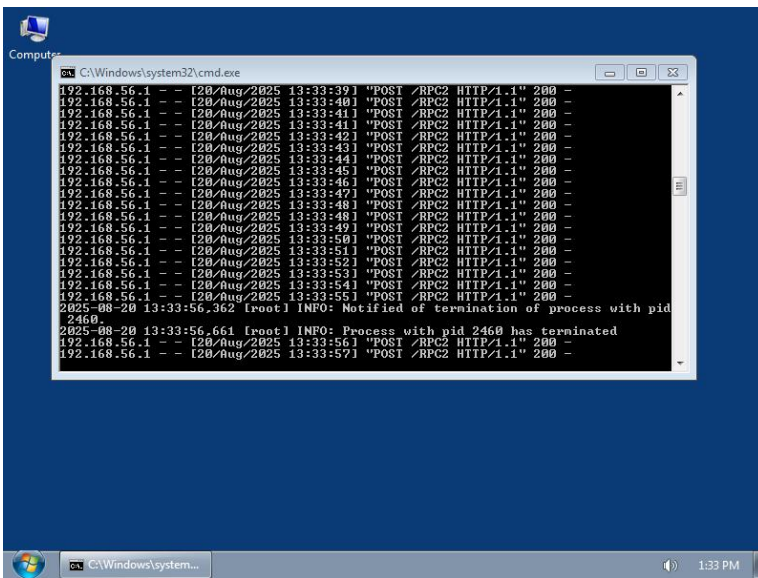
```

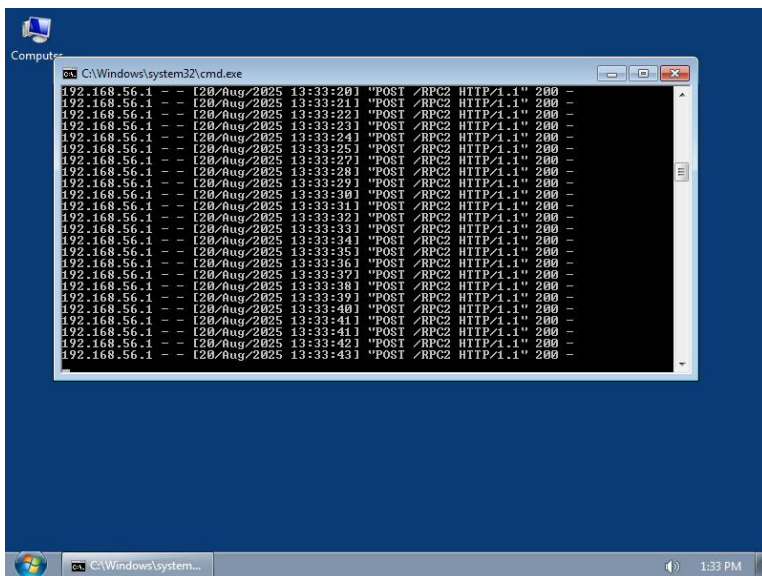
```

Computers
C:\Windows\system32\cmd.exe

2025-08-20 13:32:39.280 [lib.api.process] INFO: Successfully executed process fr
on path "C:\Users\User\AppData\Local\Temp\198808e07a5ff1f81792f5d8ad348117d57331
ee.exe" with arguments "" with pid 2460
2025-08-20 13:32:39.280 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2460
192.168.56.1 - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckoonon successfully loaded in process wi
th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -

```





```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:30] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:22] "POST /RPC2 HTTP/1.1" 200 -

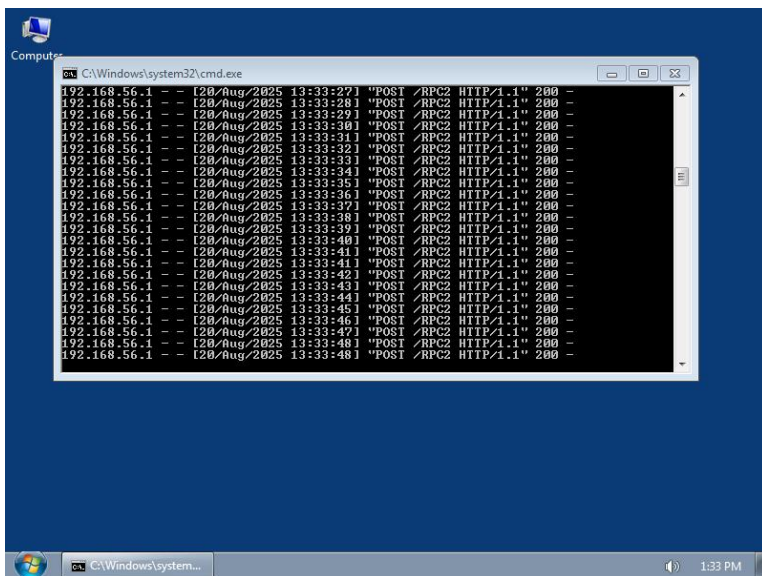
```

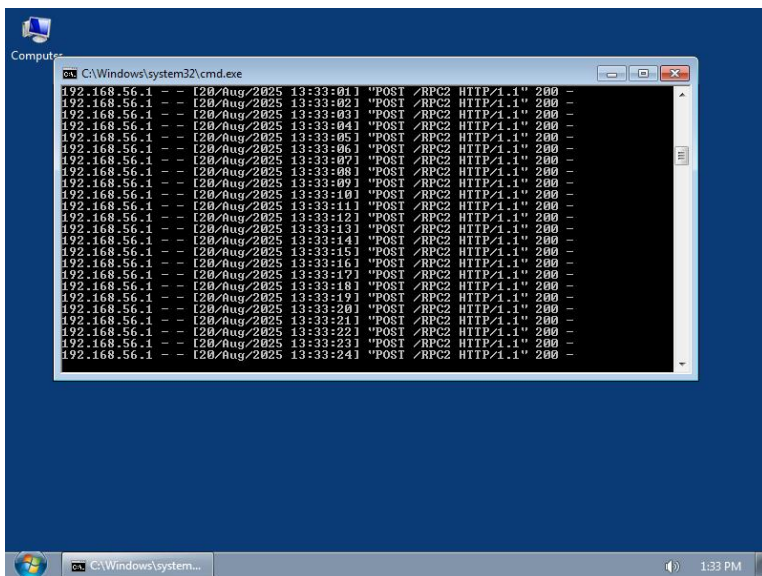
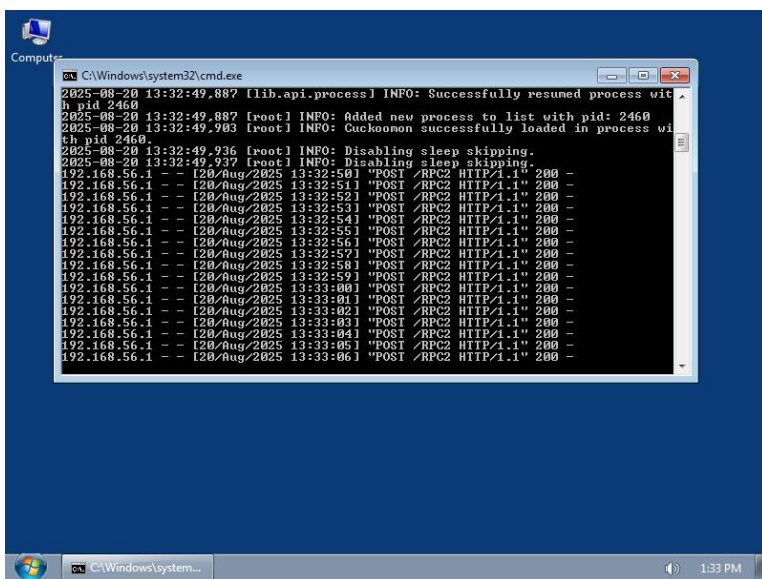
```

Computers
C:\Windows\system32\cmd.exe

2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Screenshots
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Usage
2025-08-20 13:32:39.280 [lib.api.process] INFO: Successfully executed process fr
on path "C:\Users\User\AppData\Local\Temp\198808e07a5ff1f81792f5d8ad348117d57331
ee.exe" with arguments "" with pid 2460
2025-08-20 13:32:39.280 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2460
192.168.56.1 - - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:40] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckooon successfully loaded in process wi
th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.927 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -

```





hpid 2460

```

2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckoooon successfully loaded in process wi
th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -

```

Computers

C:\Windows\system32\cmd.exe

Name	Date	Time	Size	Type
192.168.56.1	12/08/2025	13:33:17	1 KB	POST
192.168.56.1	12/08/2025	13:33:18	1 KB	POST
192.168.56.1	12/08/2025	13:33:19	1 KB	POST
192.168.56.1	12/08/2025	13:33:20	1 KB	POST
192.168.56.1	12/08/2025	13:33:21	1 KB	POST
192.168.56.1	12/08/2025	13:33:22	1 KB	POST
192.168.56.1	12/08/2025	13:33:23	1 KB	POST
192.168.56.1	12/08/2025	13:33:24	1 KB	POST
192.168.56.1	12/08/2025	13:33:25	1 KB	POST
192.168.56.1	12/08/2025	13:33:27	1 KB	POST
192.168.56.1	12/08/2025	13:33:28	1 KB	POST
192.168.56.1	12/08/2025	13:33:29	1 KB	POST
192.168.56.1	12/08/2025	13:33:30	1 KB	POST
192.168.56.1	12/08/2025	13:33:31	1 KB	POST
192.168.56.1	12/08/2025	13:33:32	1 KB	POST
192.168.56.1	12/08/2025	13:33:33	1 KB	POST
192.168.56.1	12/08/2025	13:33:34	1 KB	POST
192.168.56.1	12/08/2025	13:33:35	1 KB	POST
192.168.56.1	12/08/2025	13:33:36	1 KB	POST
192.168.56.1	12/08/2025	13:33:37	1 KB	POST
192.168.56.1	12/08/2025	13:33:38	1 KB	POST
192.168.56.1	12/08/2025	13:33:39	1 KB	POST
192.168.56.1	12/08/2025	13:33:40	1 KB	POST
192.168.56.1	12/08/2025	13:33:41	1 KB	POST

C:\Windows\system...

1:33 PM

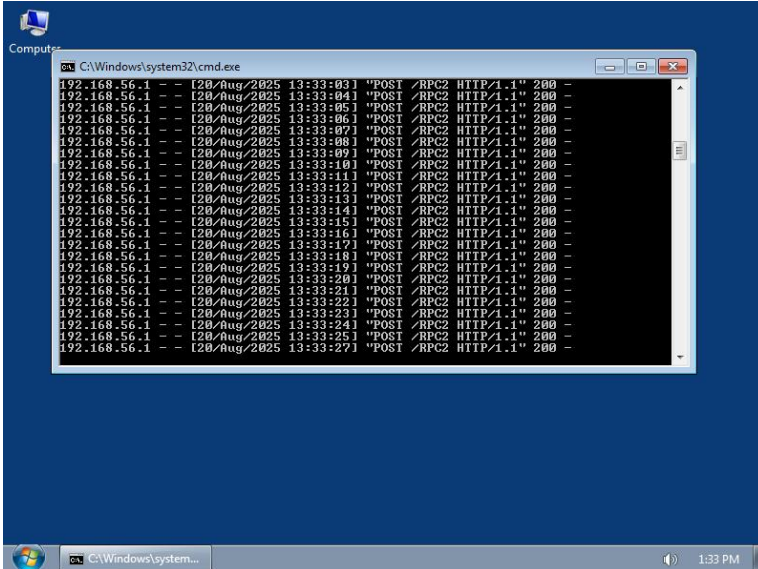
Computers

C:\Windows\system32\cmd.exe

Name	Date	Type
192.168.56.1	12/08/2025	13:33:001 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:011 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:021 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:031 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:041 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:051 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:061 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:071 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:081 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:091 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:101 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:111 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:121 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:131 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:141 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:151 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:161 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:171 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:181 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:191 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:201 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:211 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:221 POST /RPC2 HTTP/1.1
192.168.56.1	12/08/2025	13:33:231 POST /RPC2 HTTP/1.1

C:\Windows\system...

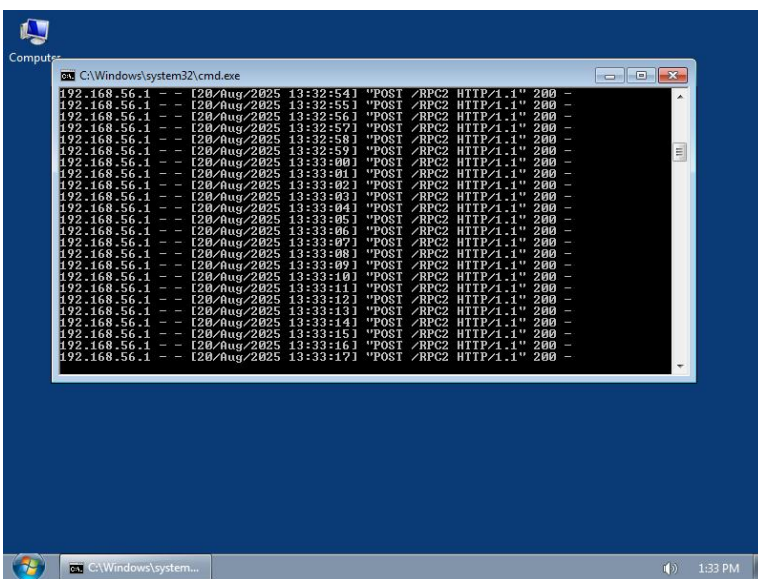
1:33 PM



```

C:\Windows\system32\cmd.exe
192.168.56.1 - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:27] "POST /RPC2 HTTP/1.1" 200 -

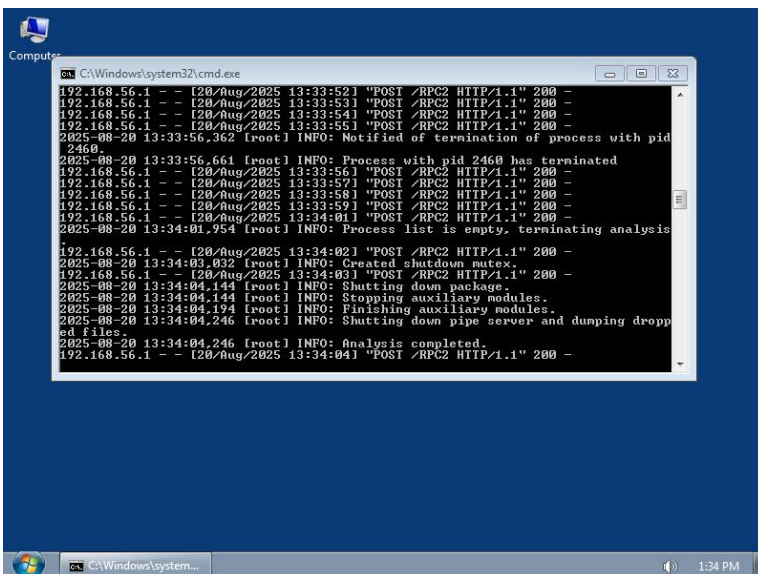
```



```

C:\Windows\system32\cmd.exe
192.168.56.1 - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -

```



```

C:\Windows\system32\cmd.exe
192.168.56.1 - [20/Aug/2025 13:33:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:55] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:33:56.362 [root] INFO: Notified of termination of process with pid 2460
2025-08-20 13:33:56.661 [root] INFO: Process with pid 2460 has terminated
192.168.56.1 - [20/Aug/2025 13:33:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:34:01] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:34:01.954 [root] INFO: Process list is empty, terminating analysis
192.168.56.1 - [20/Aug/2025 13:34:02] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:34:03.032 [root] INFO: Created shutdown mutex.
192.168.56.1 - [20/Aug/2025 13:34:03] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:34:04.144 [root] INFO: Shutting down package.
2025-08-20 13:34:04.144 [root] INFO: Stopping auxiliary modules.
2025-08-20 13:34:04.144 [root] INFO: Finishing auxiliary modules.
2025-08-20 13:34:04.246 [root] INFO: Shutting down pipe server and dumping dropped files.
2025-08-20 13:34:04.246 [root] INFO: Analysis completed.
192.168.56.1 - [20/Aug/2025 13:34:04] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - - [20/Aug/2025 13:33:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:55] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:33:56.362 [root] INFO: Notified of termination of process with pid
2460.
2025-08-20 13:33:56.661 [root] INFO: Process with pid 2460 has terminated
192.168.56.1 - - [20/Aug/2025 13:33:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:34:01] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:34:01.954 [root] INFO: Process list is empty, terminating analysis
.
  
```

```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:21] "POST /RPC2 HTTP/1.1" 200 -
  
```

```

Computers
C:\Windows\system32\cmd.exe

2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2460
192.168.56.1 - - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckoonon successfully loaded in process wi
th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
  
```

```

C:\Windows\system32\cmd.exe
2025-08-20 13:32:39.280 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit p
process with pid 2460
192.168.56.1 - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckooon successfully loaded in process wi
th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -

```

```

C:\Windows\system32\cmd.exe
192.168.56.1 - [20/Aug/2025 13:33:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:52] "POST /RPC2 HTTP/1.1" 200 -

```

```

C:\Windows\system32\cmd.exe
192.168.56.1 - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:20] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:25] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

2025-08-20 13:32:39.203 [root] DEBUG: Started auxiliary module Browser
2025-08-20 13:32:39.203 [modules.auxiliary.digisig] INFO: Skipping authenticode
validation, signtool.exe was not found in bin/
2025-08-20 13:32:39.203 [root] DEBUG: Started auxiliary module DigiSig
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Disguise
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Human
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Screenshots
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Usage
2025-08-20 13:32:39.280 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\User\AppData\Local\Temp\198808e07a5ff1f81792f5d8ad348117d57331
ee.exe" with arguments with pid 2460
2025-08-20 13:32:39.280 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2460
192.168.56.1 - - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckooon successfully loaded in process wi
th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe

192.168.56.1 - - [20/Aug/2025 13:33:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:55] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:33:56.362 [root] INFO: Notified of termination of process with pid
2460
2025-08-20 13:33:56.661 [root] INFO: Process with pid 2460 has terminated
192.168.56.1 - - [20/Aug/2025 13:33:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:34:01] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:34:01.954 [root] INFO: Process list is empty, terminating analysis
192.168.56.1 - - [20/Aug/2025 13:34:02] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:34:03.032 [root] INFO: Created shutdown mutex.
192.168.56.1 - - [20/Aug/2025 13:34:03] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckooon successfully loaded in process wi
ch pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -

```

```

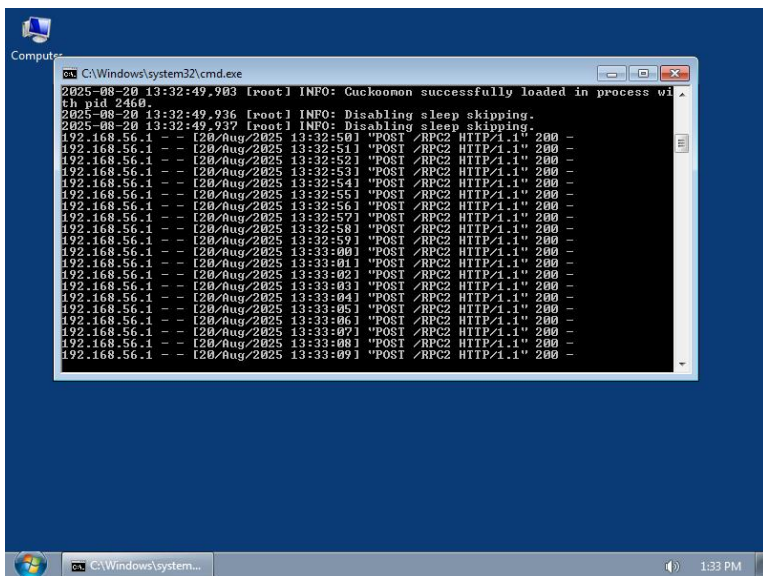
Computers
C:\Windows\system32\cmd.exe
192.168.56.1 - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -

```

```

Computers
C:\Windows\system32\cmd.exe
192.168.56.1 - [20/Aug/2025 13:33:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:55] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:33:56.362 [root] INFO: Notified of termination of process with pid
2460.
2025-08-20 13:33:56.661 [root] INFO: Process with pid 2460 has terminated
192.168.56.1 - [20/Aug/2025 13:33:56] "POST /RPC2 HTTP/1.1" 200 -

```



```

Computers
C:\Windows\system32\cmd.exe
192.168.56.1 - [20/Aug/2025 13:33:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:32] "POST /RPC2 HTTP/1.1" 200 -
  
```

```

Computers
C:\Windows\system32\cmd.exe
192.168.56.1 - [20/Aug/2025 13:33:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:55] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:33:56.362 [root] INFO: Notified of termination of process with pid
2460
2025-08-20 13:33:56.661 [root] INFO: Process with pid 2460 has terminated
192.168.56.1 - [20/Aug/2025 13:33:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:59] "POST /RPC2 HTTP/1.1" 200 -
  
```

```

Computers
C:\Windows\system32\cmd.exe
192.168.56.1 - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckoonon successfully loaded in process wi
th pid 2460
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - [20/Aug/2025 13:33:05] "POST /RPC2 HTTP/1.1" 200 -
  
```

```

C:\Windows\system32\cmd.exe
2025-08-20 13:32:39.203 [root] DEBUG: Started auxiliary module Browser
2025-08-20 13:32:39.203 [modules.auxiliary.digisig] INFO: Skipping authenticode
validation. signtool.exe was not found in bin/
2025-08-20 13:32:39.203 [root] DEBUG: Started auxiliary module DigiSig
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Disguise
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Human
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Screenshots
2025-08-20 13:32:39.217 [root] DEBUG: Started auxiliary module Usage
2025-08-20 13:32:39.200 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\User\AppData\Local\Temp\198808e07a5ff1f81792f5d8ad348117d57331
ee.exe" with arguments "" with pid 2460
2025-08-20 13:32:39.200 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2460
192.168.56.1 - - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckoonon successfully loaded in process wi
th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.

```

```

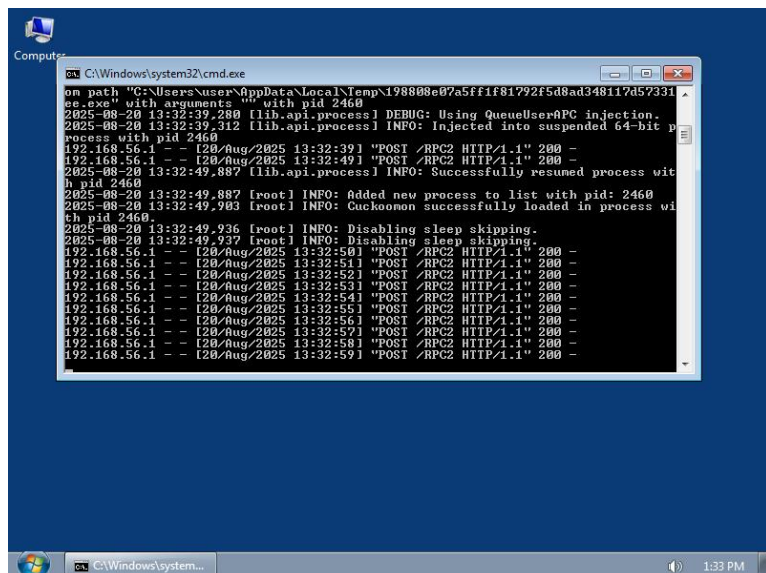
C:\Windows\system32\cmd.exe
process with pid 2460
192.168.56.1 - - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckoonon successfully loaded in process wi
th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.937 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:03] "POST /RPC2 HTTP/1.1" 200 -

```

```

C:\Windows\system32\cmd.exe
192.168.56.1 - - [20/Aug/2025 13:33:14] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:20] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:22] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:33] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:33:38] "POST /RPC2 HTTP/1.1" 200 -

```



```

C:\Windows\system32\cmd.exe
on path "C:\Users\User\AppData\Local\Temp\198808e07a5ff1f81792f5d8ad348117d57331
ee.exe" with arguments "" with pid 2460
2025-08-20 13:32:39.280 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-08-20 13:32:39.312 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2460
192.168.56.1 - - [20/Aug/2025 13:32:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:49] "POST /RPC2 HTTP/1.1" 200 -
2025-08-20 13:32:49.887 [lib.api.process] INFO: Successfully resumed process wit
h pid 2460
2025-08-20 13:32:49.887 [root] INFO: Added new process to list with pid: 2460
2025-08-20 13:32:49.903 [root] INFO: Cuckoonon successfully loaded in process wi
th pid 2460.
2025-08-20 13:32:49.936 [root] INFO: Disabling sleep skipping.
2025-08-20 13:32:49.977 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [20/Aug/2025 13:32:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [20/Aug/2025 13:32:59] "POST /RPC2 HTTP/1.1" 200 -
  
```