Summary

File Name: f.exe

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

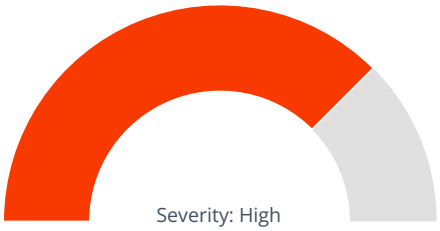
SHA1: 61817e25b0cfae37a3f289fc308e67146f874342

MD5: 7b910a871a5bb36d8f47094f51eaac46

MALWARE

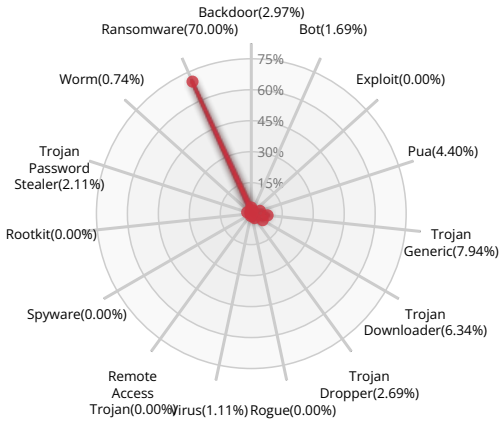
Valkyrie Final Verdict

DETECTION SECTION

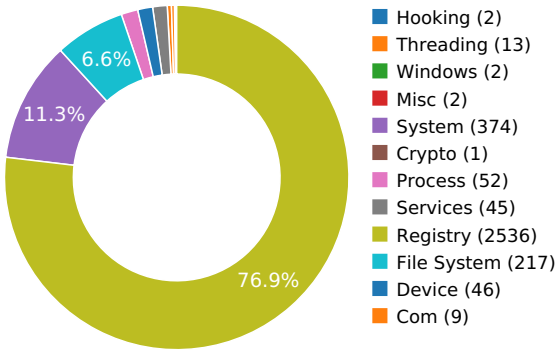


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

SPAM, UNWANTED ADVERTISEMENTS AND RANSOM DEMANDS

Attempts to delete volume shadow copies Show sources

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

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
\??\MountPointManager
C:\
D:\
C:\$Recycle.Bin\S-1-5-21-2298303332-66077612-2598613238-1000
C:\$Recycle.Bin\S-1-5-21-2298303332-66077612-2598613238-1000\desktop.ini
C:\$Recycle.Bin\S-1-5-21-2298303332-66077612-2598613238-1000\$R*.*
D:\$RECYCLE.BIN
D:\$RECYCLE.BIN\desktop.ini
D:\$RECYCLE.BIN\$R*.*
C:\Users\user\AppData\Local\Temp
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp\vssadmin.exe
C:\Users\user\AppData\Local\Temp\vssadmin.exe.*
C:\ProgramData\Oracle\Java\javapath\vssadmin.exe
C:\ProgramData\Oracle\Java\javapath\vssadmin.exe.*
C:\Windows\sysnative\vssadmin.exe
\Device\KsecDD

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\MaxCapacity
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\NukeOnDelete
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\MaxCapacity
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\NukeOnDelete
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\RecycleBinDrives
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\ParentFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\FolderTypeID

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\InitFolderHandler

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Category

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Name

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\ParentFolder

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Description

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\RelativePath

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\ParsingName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\InfoTip

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\LocalizedName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Icon

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Security

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\StreamResource

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\StreamResourceType

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\LocalRedirectOnly

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Roamable

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PreCreate

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Stream

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PublishExpandedPath

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Attributes

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\FolderTypeID

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\InitFolderHandler

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\Category

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\Name

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\ParentFolder

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\InitFolderHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{2112AB0A-C86A-4FFE-A368-0DE96E47012E}\Category

RESOLVED APIS

cryptsp.dll.CryptAcquireContextW
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
kernel32.dll.IsWow64Process
kernel32.dll.Wow64DisableWow64FsRedirection
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW

setupapi.dll.CM_Get_Device_Interface_List_ExW
comctl32.dll.#386
kernel32.dll.Wow64RevertWow64FsRedirection
shell32.dll.#66
comctl32.dll.#326
comctl32.dll.#321
advapi32.dll.GetNamedSecurityInfoW
sechost.dll.ConvertStringSecurityDescriptorToSecurityDescriptorW
comctl32.dll.#339
advapi32.dll.UnregisterTraceGuids
kernel32.dll.SetThreadUILanguage
kernel32.dll.CopyFileExW
kernel32.dll.IsDebuggerPresent
kernel32.dll.SetConsoleInputExeNameW
cryptbase.dll.SystemFunction036
sechost.dll.LookupAccountNameLocalW
advapi32.dll.LookupAccountSidW
sechost.dll.LookupAccountSidLocalW
oleaut32.dll.#500
cryptsp.dll.CryptReleaseContext

REGISTRY KEYS

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\CurrentVersion\ShellCompatibility\Applications\61817e25b0cfae37a3f289fc308e67146f874342.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\MaxCapacity
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\NukeOnDelete
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\MaxCapacity
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\BitBucket\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\NukeOnDelete
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\RecycleBinDrives
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\ParentFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\StreamResource

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\StreamResourceType

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\LocalRedirectOnly

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Roamable

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\PreCreate

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Stream

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\PublishExpandedPath

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\Attributes

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\FolderTypeID

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\InitFolderHandler

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{7D1D3A04-DEBB-4115-95CF-2F29DA2920DA}\PropertyBag

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Category

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Name

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\ParentFolder

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Description

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\RelativePath

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\ParsingName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\InfoTip

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\LocalizedName

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Icon

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Security

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\StreamResource

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\StreamResourceType

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\LocalRedirectOnly

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\InitFolderHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PropertyBag
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{F7F1ED05-9F6D-47A2-AAAE-29D317C6F066}\ParentFolder

EXECUTED COMMANDS

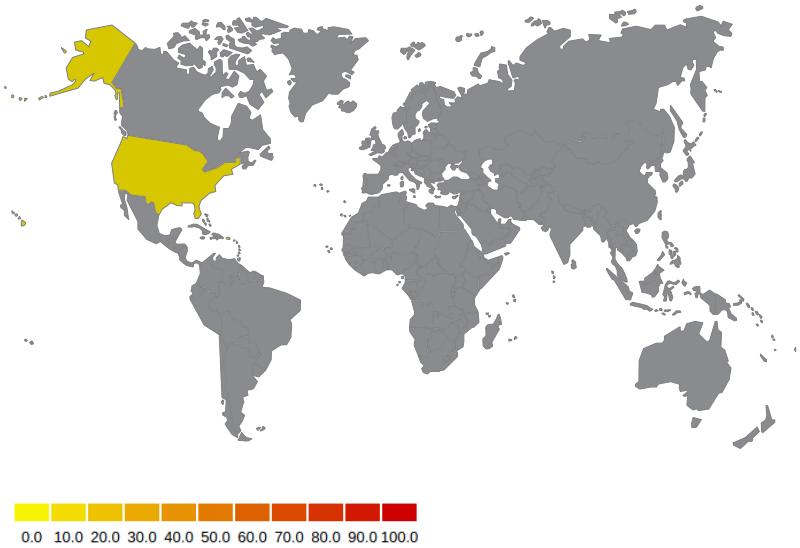
cmd.exe /c vssadmin.exe delete shadows /all /quiet
vssadmin.exe delete shadows /all /quiet

READ FILES

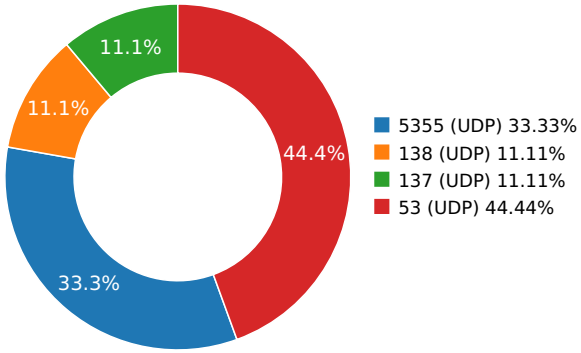
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\$Recycle.Bin\S-1-5-21-2298303332-66077612-2598613238-1000\desktop.ini
D:\$RECYCLE.BIN\desktop.ini
\Device\KsecDD

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Google LLC	Malware Process
	8.8.8.8	United States	15169	Google LLC	Malware Process
					Malware Process
www.aieov.com	45.56.79.23	United States	63949	Akamai Technologies, Inc.	Malware Process

DNS QUERIES

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

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.03733992577	Sandbox	224.0.0.252	5355
7.03794002533	Sandbox	224.0.0.252	5355
7.07911705971	Sandbox	192.168.56.255	137
9.60918998718	Sandbox	224.0.0.252	5355
10.3752291203	Sandbox	8.8.4.4	53
11.3744149208	Sandbox	8.8.8.8	53
13.1352450848	Sandbox	192.168.56.255	138
24.7522649765	Sandbox	8.8.8.8	53
25.7495319843	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	f.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	61817e25b0cfae37a3f289fc308e67146f874342
MD5:	7b910a871a5bb36d8f47094f51eaac46
First Seen Date:	2024-05-12 19:35:34.841516 (a day ago)
Number Of Clients Seen:	4
Last Analysis Date:	2024-05-12 19:36:31.732640 (a day ago)
Human Expert Analysis Date:	2024-05-13 17:04:51.246728 (about 7 hours ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[]
Compilation Time Stamp	0x6615903F [Tue Apr 9 19:00:15 2024 UTC]
Entry Point	0x40ac30 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	80896
Ssdeep	
Sha256	ae2b65de86e012e926c22d0f81c7d4e495d8cbcae8aa34c298c267477d2d3ec0
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

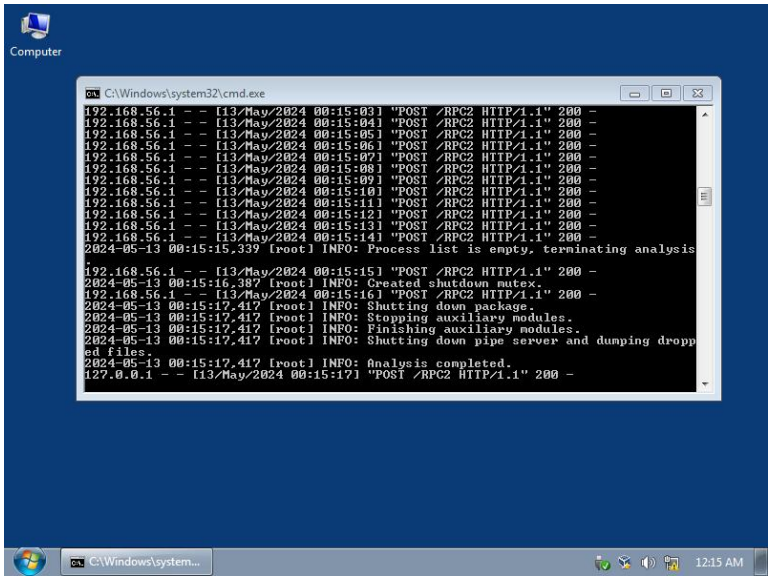
PE Sections

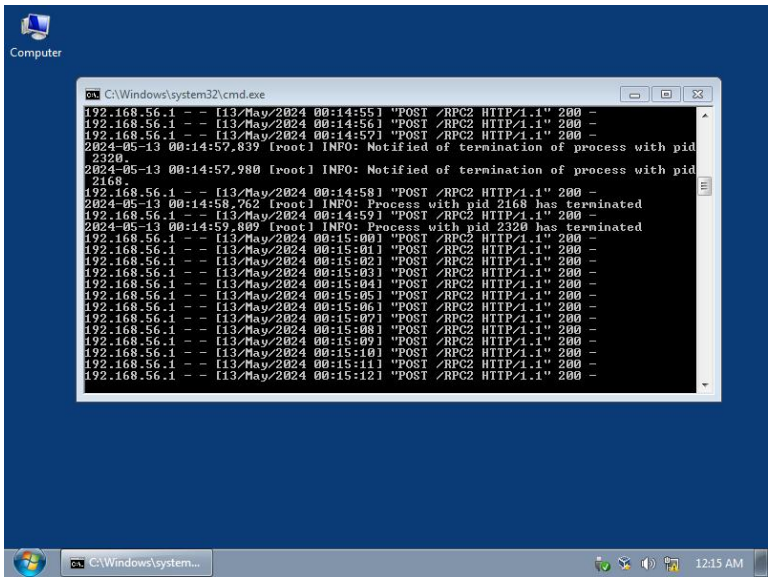
NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x122e7	0x12400	5.90987757538	3f1406a4437e8f0cff9c28dfe3f130f9
.data	0x14000	0x268	0x200	4.20051959504	983a1e13bda53f5dd0a3a01ce6ded159
.idata	0x15000	0x97a	0xa00	5.09718074777	c3c925ff9e1780c2fa613ea337521208
.CRT	0x16000	0x8	0x200	0.0940979256627	efee18195bb108622b35df0104b325bd
.reloc	0x17000	0x418	0x600	5.08891192378	e06542aef564d381d8d2db6434d1890e

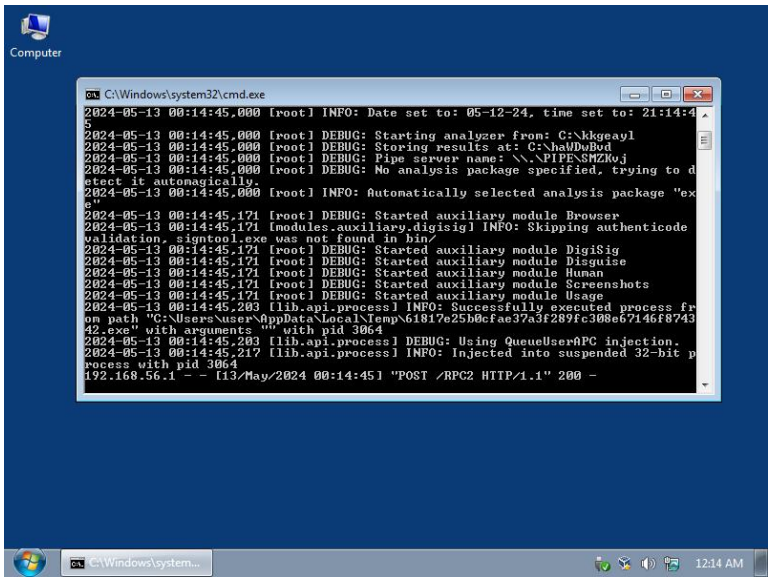
CERTIFICATE VALIDATION

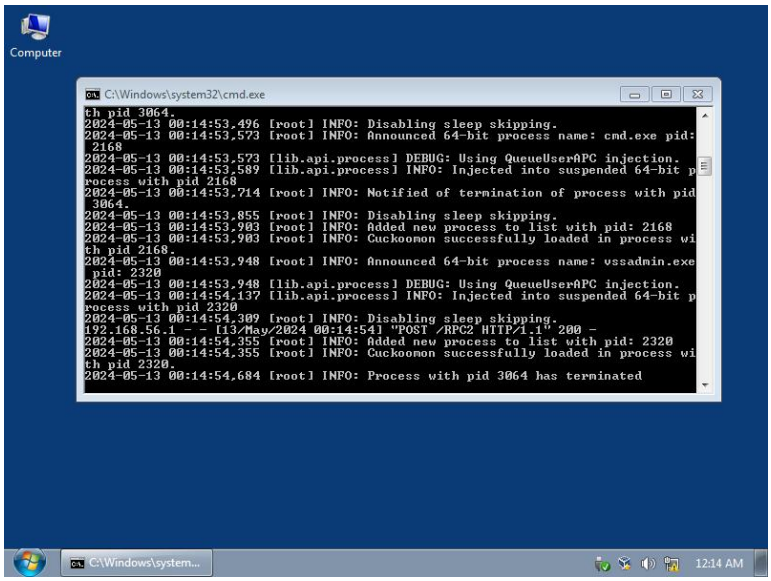
- Certificate Validation is not Applicable ?

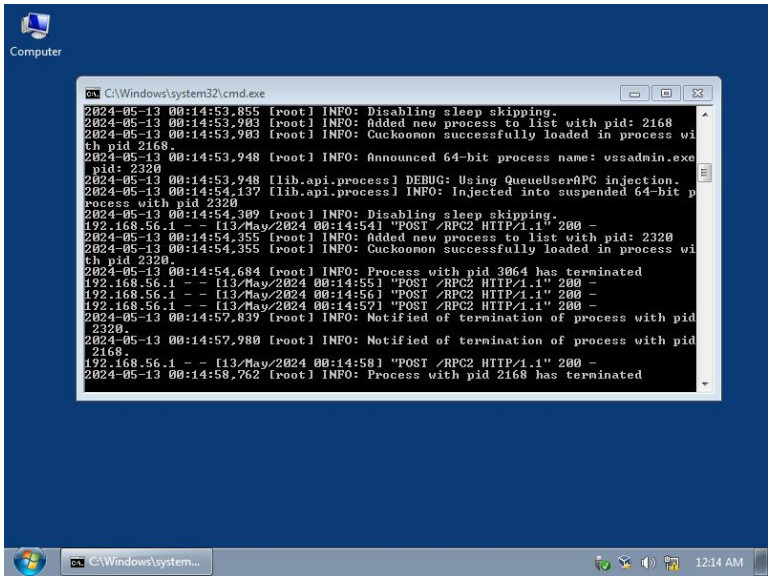
SCREENSHOTS

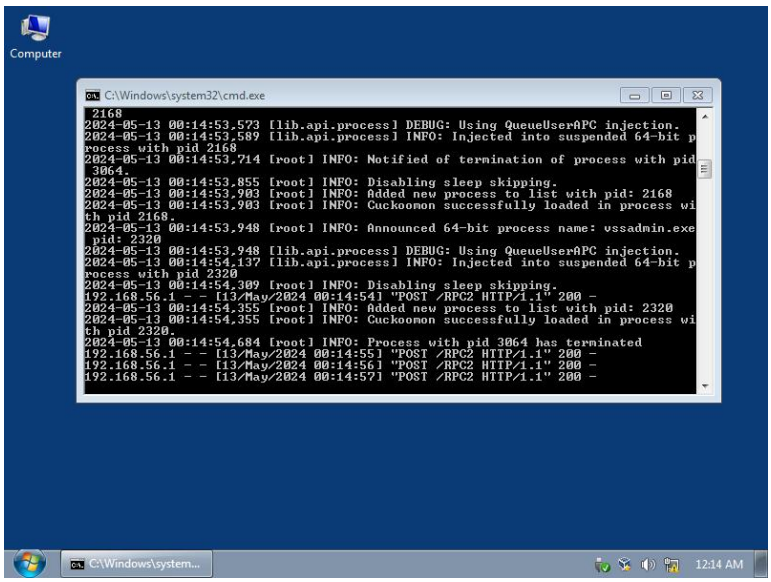

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:14] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:15:15,339 [root] INFO: Process list is empty, terminating analysis
.
192.168.56.1 - - [13/May/2024 00:15:15] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:15:16,387 [root] INFO: Created shutdown mutex.
192.168.56.1 - - [13/May/2024 00:15:16] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:15:17,417 [root] INFO: Shutting down package.
2024-05-13 00:15:17,417 [root] INFO: Stopping auxiliary modules.
2024-05-13 00:15:17,417 [root] INFO: Finishing auxiliary modules.
2024-05-13 00:15:17,417 [root] INFO: Shutting down pipe server and dumping dropp
ed files.
2024-05-13 00:15:17,417 [root] INFO: Analysis completed.
127.0.0.1 - - [13/May/2024 00:15:17] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM

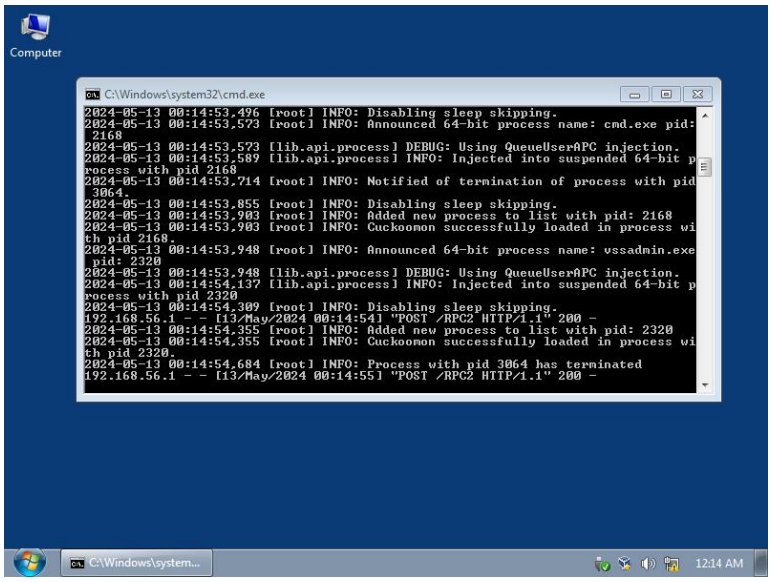

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid
2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid
2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:12] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM

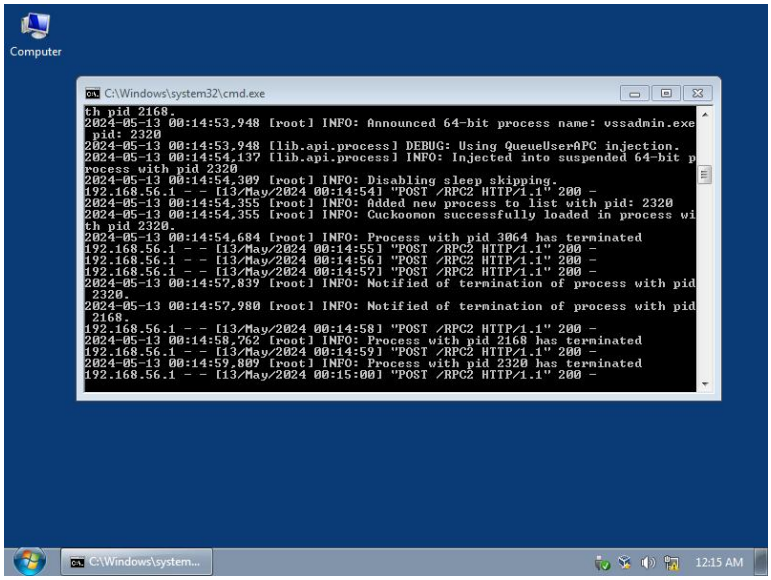

Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:45,000 [root] INFO: Date set to: 05-12-24, time set to: 21:14:4
5
2024-05-13 00:14:45,000 [root] DEBUG: Starting analyzer from: C:\kkgeayl
2024-05-13 00:14:45,000 [root] DEBUG: Storing results at: C:\haVDwBvd
2024-05-13 00:14:45,000 [root] DEBUG: Pipe server name: \\.\PIPE\SMZKvj
2024-05-13 00:14:45,000 [root] DEBUG: No analysis package specified, trying to d
etect it automagically.
2024-05-13 00:14:45,000 [root] INFO: Automatically selected analysis package "ex
e"
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Browser
2024-05-13 00:14:45,171 [modules.auxiliary.digisig] INFO: Skipping authenticode
validation, signtool.exe was not found in bin/
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module DigiSig
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Disguise
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Human
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Screenshots
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Usage
2024-05-13 00:14:45,203 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\61817e25b0cfae37a3f289fc308e67146f8743
42.exe" with arguments "" with pid 3064
2024-05-13 00:14:45,203 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:45,217 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3064
192.168.56.1 - - [13/May/2024 00:14:45] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:14 AM

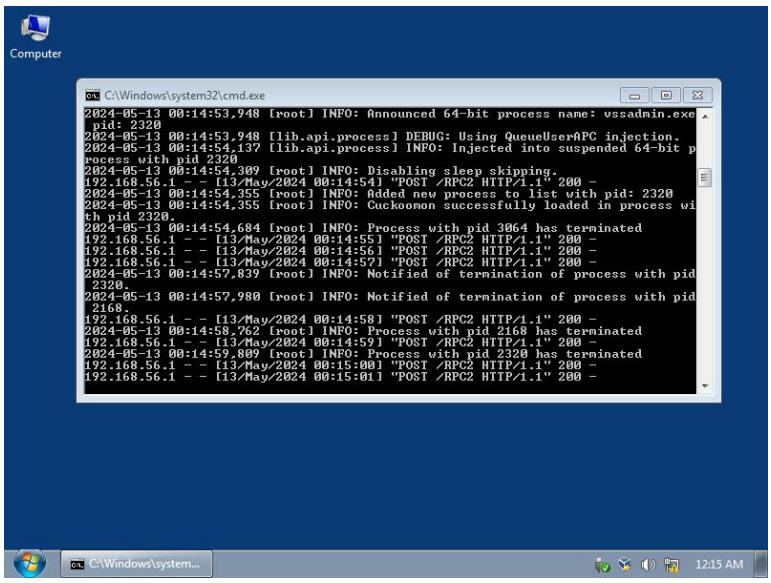

Computer
C:\Windows\system32\cmd.exe
th pid 3064.
2024-05-13 00:14:53,496 [root] INFO: Disabling sleep skipping.
2024-05-13 00:14:53,573 [root] INFO: Announced 64-bit process name: cmd.exe pid:
2168
2024-05-13 00:14:53,573 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:53,589 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2168
2024-05-13 00:14:53,714 [root] INFO: Notified of termination of process with pid
3064.
2024-05-13 00:14:53,855 [root] INFO: Disabling sleep skipping.
2024-05-13 00:14:53,903 [root] INFO: Added new process to list with pid: 2168
2024-05-13 00:14:53,903 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2168.
2024-05-13 00:14:53,948 [root] INFO: Announced 64-bit process name: vssadmin.exe
pid: 2320
2024-05-13 00:14:53,948 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:54,137 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2320
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
C:\Windows\system...
12:14 AM

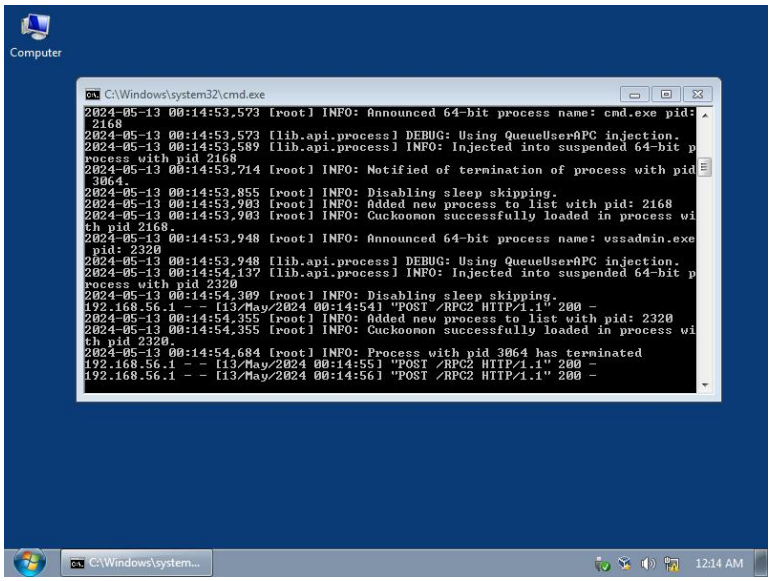

Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:53,855 [root] INFO: Disabling sleep skipping.
2024-05-13 00:14:53,903 [root] INFO: Added new process to list with pid: 2168
2024-05-13 00:14:53,903 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2168.
2024-05-13 00:14:53,948 [root] INFO: Announced 64-bit process name: vssadmin.exe
pid: 2320
2024-05-13 00:14:53,948 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:54,137 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2320
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid
2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid
2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
C:\Windows\system...
12:14 AM

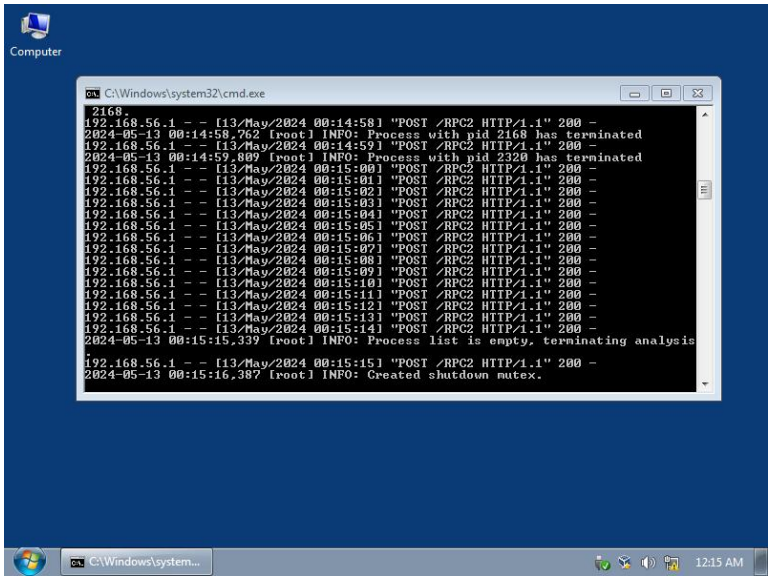

Computer
C:\Windows\system32\cmd.exe
2168
2024-05-13 00:14:53,573 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:53,589 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2168
2024-05-13 00:14:53,714 [root] INFO: Notified of termination of process with pid
3064.
2024-05-13 00:14:53,855 [root] INFO: Disabling sleep skipping.
2024-05-13 00:14:53,903 [root] INFO: Added new process to list with pid: 2168
2024-05-13 00:14:53,903 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2168.
2024-05-13 00:14:53,948 [root] INFO: Announced 64-bit process name: vssadmin.exe
pid: 2320
2024-05-13 00:14:53,948 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:54,137 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2320
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:14 AM

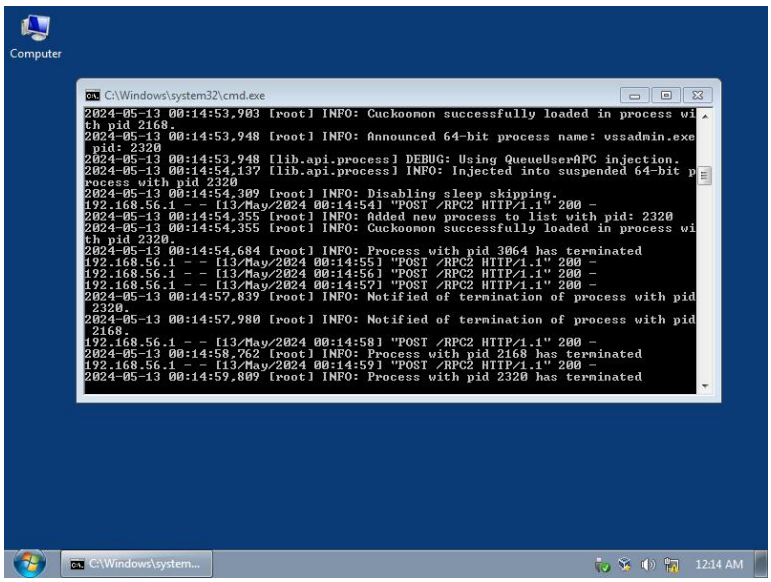

Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:53,496 [root] INFO: Disabling sleep skipping.
2024-05-13 00:14:53,573 [root] INFO: Announced 64-bit process name: cmd.exe pid: 2168
2024-05-13 00:14:53,573 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:53,589 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2168
2024-05-13 00:14:53,714 [root] INFO: Notified of termination of process with pid 3064.
2024-05-13 00:14:53,855 [root] INFO: Disabling sleep skipping.
2024-05-13 00:14:53,903 [root] INFO: Added new process to list with pid: 2168
2024-05-13 00:14:53,903 [root] INFO: Cuckoomon successfully loaded in process with pid 2168.
2024-05-13 00:14:53,948 [root] INFO: Announced 64-bit process name: vssadmin.exe pid: 2320
2024-05-13 00:14:53,948 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:54,137 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2320
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process with pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:14 AM

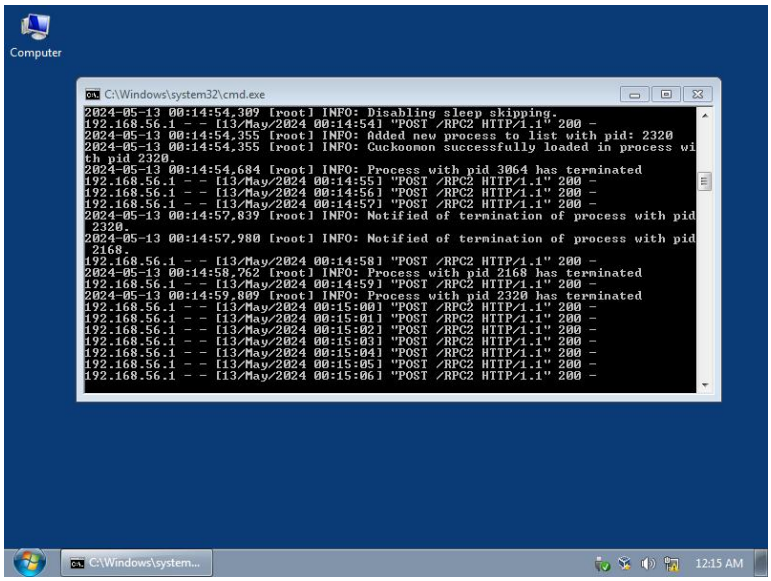

Computer
C:\Windows\system32\cmd.exe
th pid 2168.
2024-05-13 00:14:53,948 [root] INFO: Announced 64-bit process name: vssadmin.exe pid: 2320
2024-05-13 00:14:53,948 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:54,137 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2320
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process with pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid 2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid 2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM

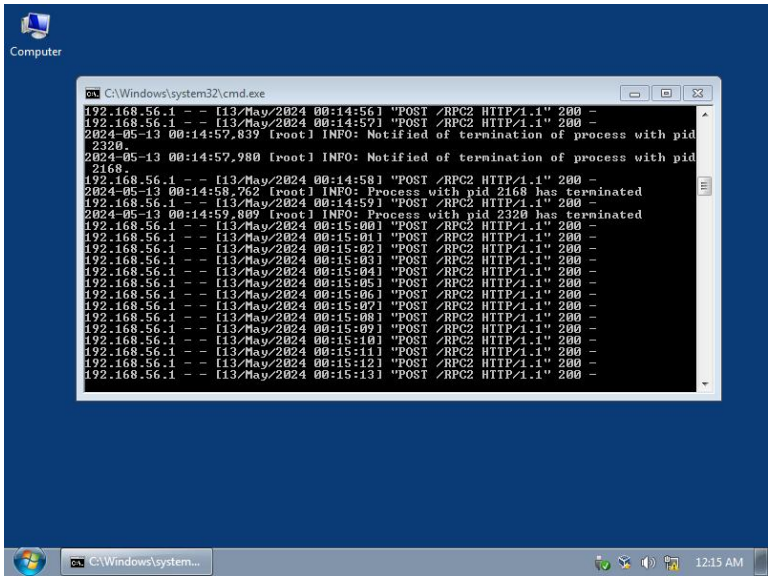

Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:53,948 [root] INFO: Announced 64-bit process name: vssadmin.exe pid: 2320
2024-05-13 00:14:53,948 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:54,137 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2320
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process with pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid 2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid 2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM

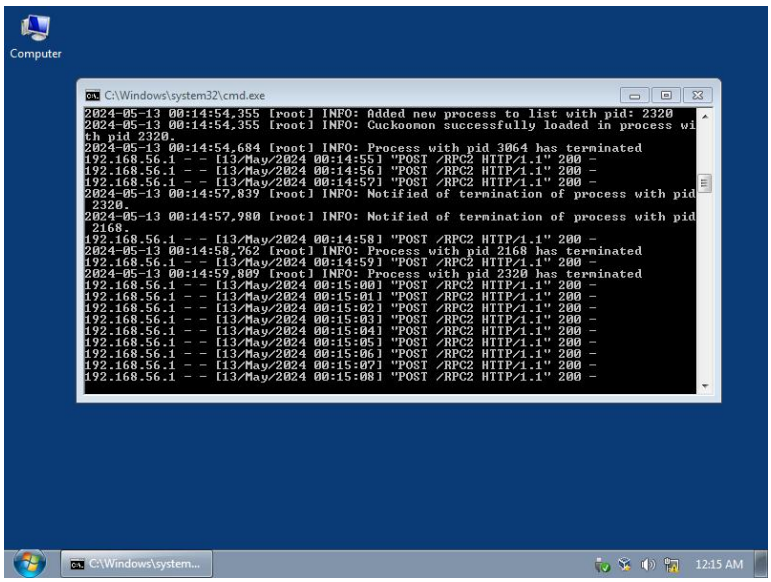

Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:53,573 [root] INFO: Announced 64-bit process name: cmd.exe pid: 2168
2024-05-13 00:14:53,573 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:53,589 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2168
2024-05-13 00:14:53,714 [root] INFO: Notified of termination of process with pid 3064.
2024-05-13 00:14:53,855 [root] INFO: Disabling sleep skipping.
2024-05-13 00:14:53,903 [root] INFO: Added new process to list with pid: 2168
2024-05-13 00:14:53,903 [root] INFO: Cuckoomon successfully loaded in process with pid 2168.
2024-05-13 00:14:53,948 [root] INFO: Announced 64-bit process name: vssadmin.exe pid: 2320
2024-05-13 00:14:53,948 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:54,137 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2320
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process with pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:14 AM

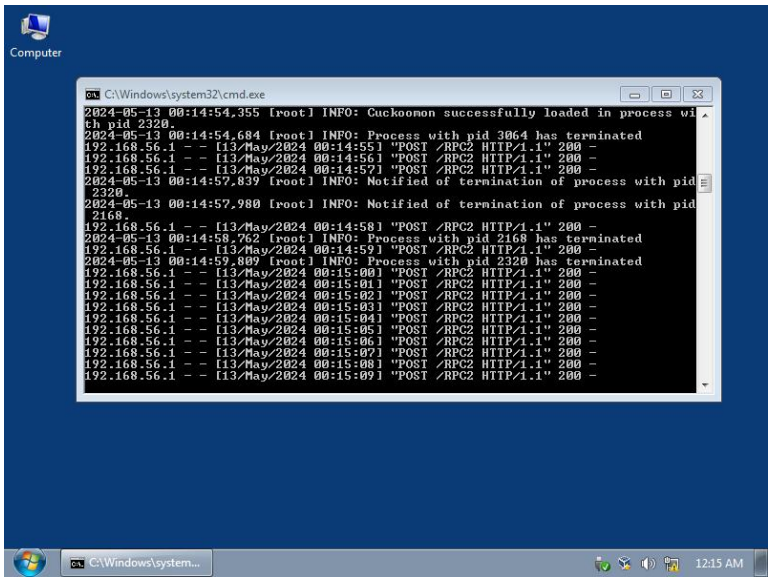

Computer
C:\Windows\system32\cmd.exe
2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:14] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:15:15,339 [root] INFO: Process list is empty, terminating analysis.
192.168.56.1 - - [13/May/2024 00:15:15] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:15:16,387 [root] INFO: Created shutdown mutex.
C:\Windows\system...
12:15 AM

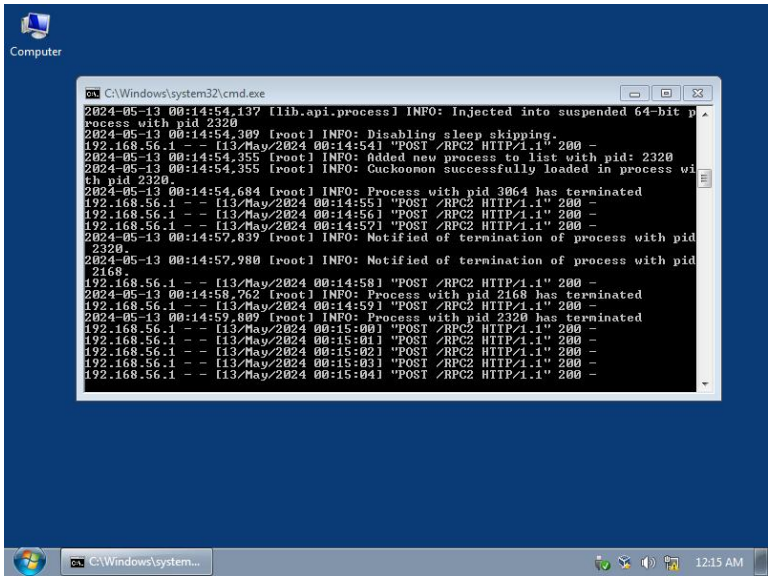

Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:53,903 [root] INFO: Cuckoomon successfully loaded in process with pid 2168.
2024-05-13 00:14:53,948 [root] INFO: Announced 64-bit process name: vssadmin.exe pid: 2320
2024-05-13 00:14:53,948 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:54,137 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2320
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process with pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid 2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid 2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
C:\Windows\system...
12:14 AM

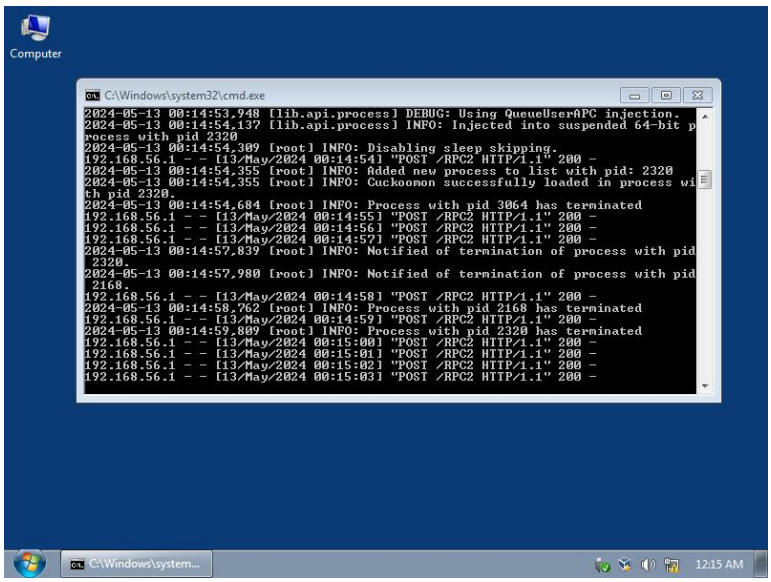

Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process with pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid 2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid 2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:06] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM

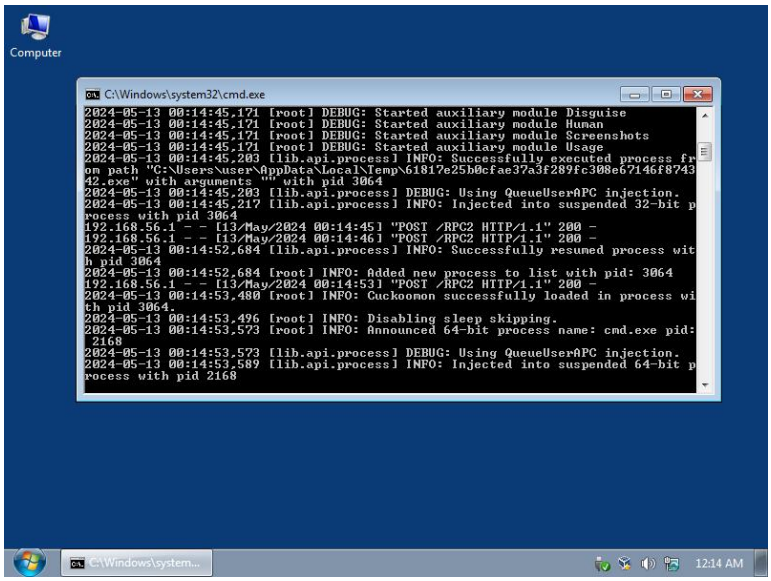

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid 2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid 2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:13] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM

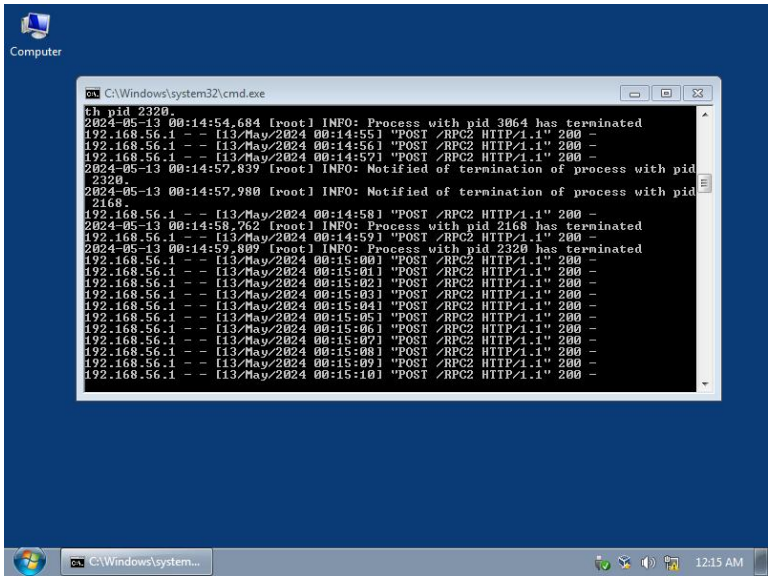

Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process with pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid 2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid 2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:08] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM

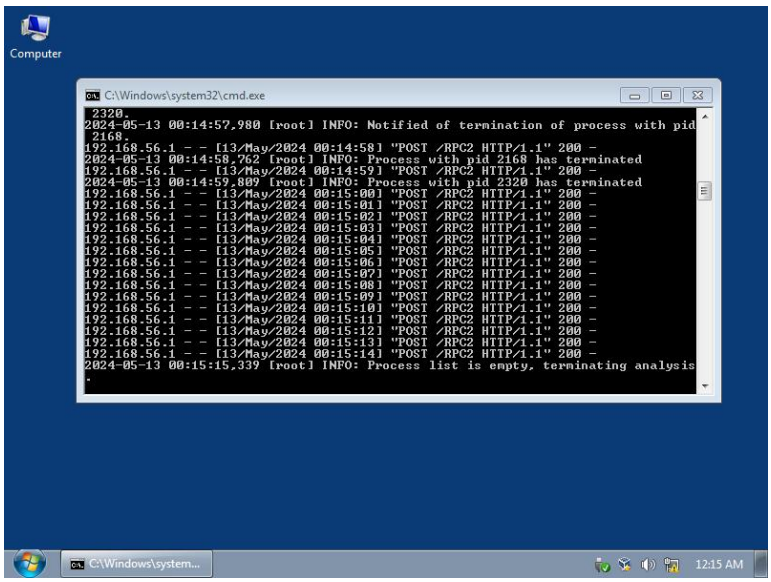

Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid
2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid
2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:09] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM

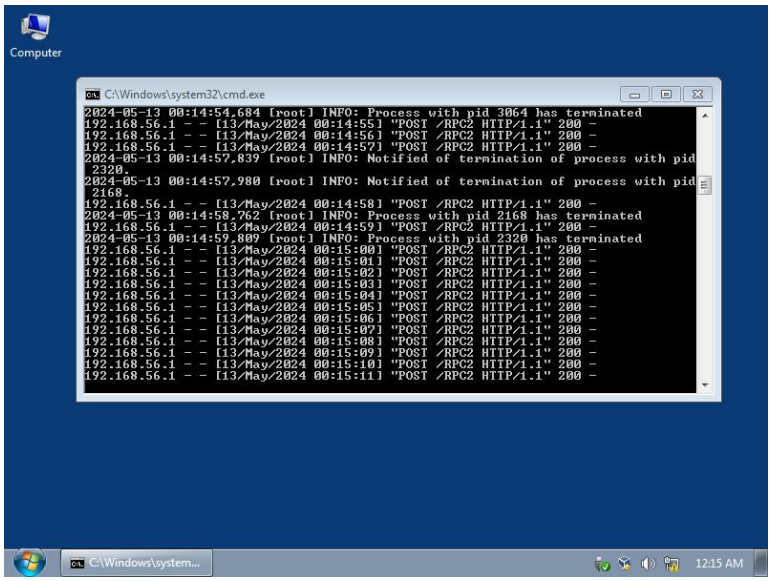

Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:54,137 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2320
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid
2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid
2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM

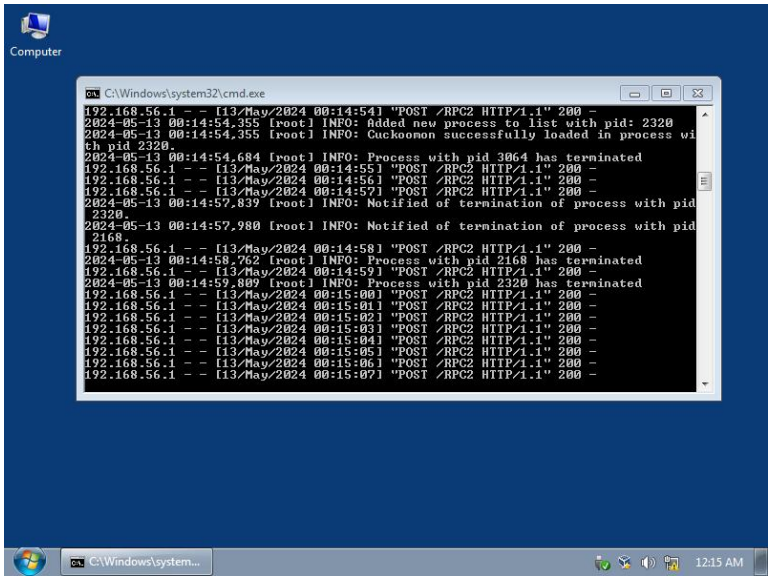

Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:53,948 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:54,137 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2320
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid
2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid
2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM

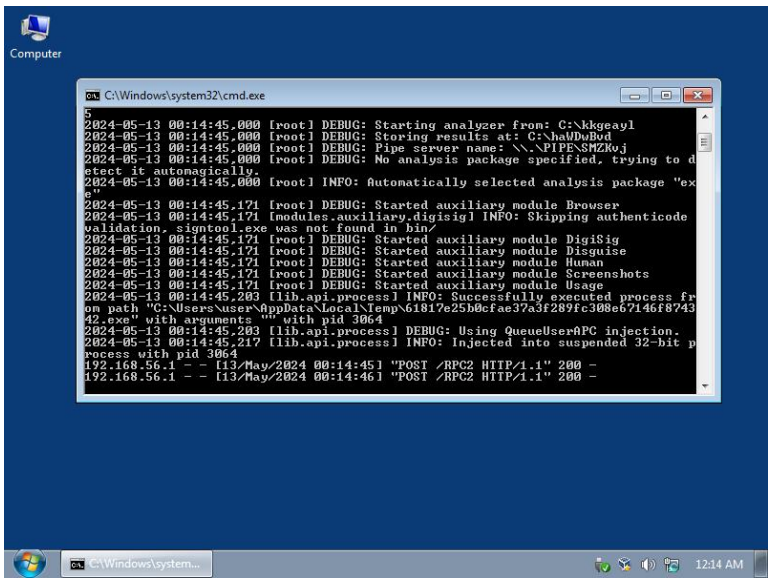

Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Disguise
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Human
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Screenshots
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Usage
2024-05-13 00:14:45,203 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\61817e25b0cfae37a3f289fc308e67146f8743
42.exe" with arguments "" with pid 3064
2024-05-13 00:14:45,203 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:45,217 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 3064
192.168.56.1 - - [13/May/2024 00:14:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:46] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:52,684 [lib.api.process] INFO: Successfully resumed process wit
h pid 3064
2024-05-13 00:14:52,684 [root] INFO: Added new process to list with pid: 3064
192.168.56.1 - - [13/May/2024 00:14:53] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:53,480 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 3064.
2024-05-13 00:14:53,496 [root] INFO: Disabling sleep skipping.
2024-05-13 00:14:53,573 [root] INFO: Announced 64-bit process name: cmd.exe pid:
2168
2024-05-13 00:14:53,573 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:53,589 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2168
C:\Windows\system...
12:14 AM

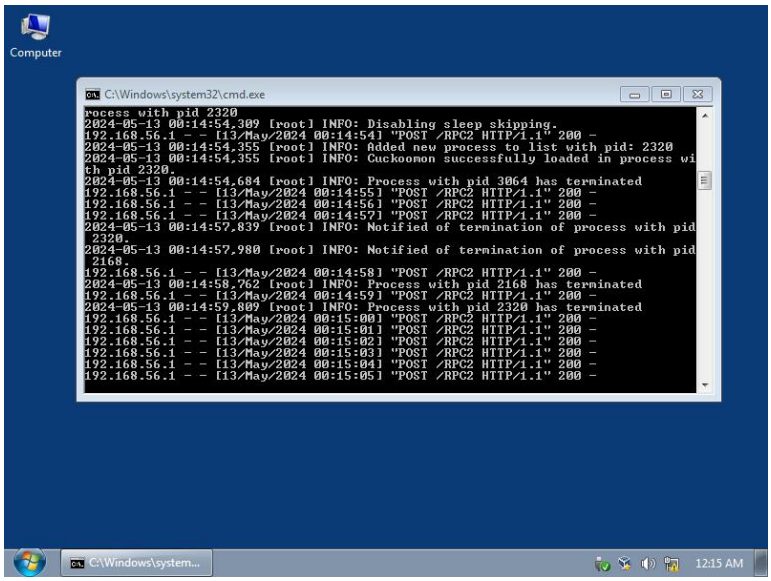

Computer
C:\Windows\system32\cmd.exe
th pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid
2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid
2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:10] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM

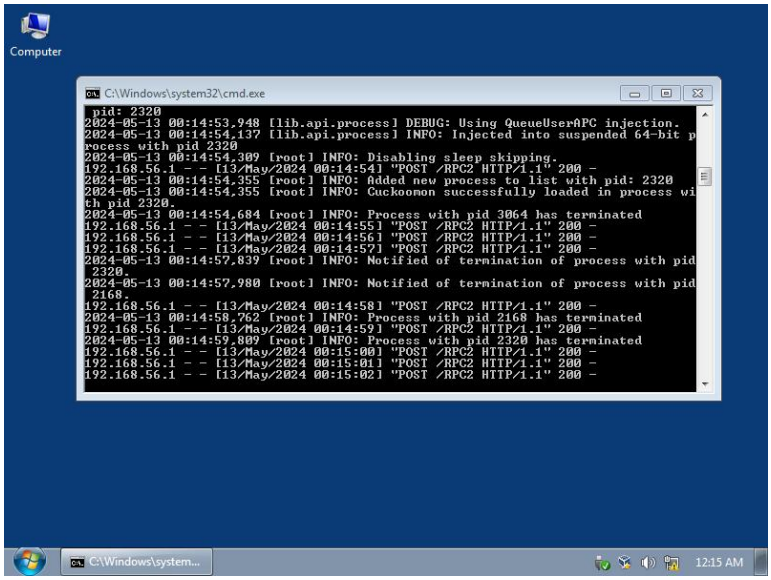

Computer
C:\Windows\system32\cmd.exe
2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid
2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:14] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:15:15,339 [root] INFO: Process list is empty, terminating analysis
.
C:\Windows\system...
12:15 AM


Computer
C:\Windows\system32\cmd.exe
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid 2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid 2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:11] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM


Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process with pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid 2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid 2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:06] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:07] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM


Computer
C:\Windows\system32\cmd.exe
S
2024-05-13 00:14:45,000 [root] DEBUG: Starting analyzer from: C:\kkgeayl
2024-05-13 00:14:45,000 [root] DEBUG: Storing results at: C:\haWDwBvd
2024-05-13 00:14:45,000 [root] DEBUG: Pipe server name: \\.\PIPE\SMZKvj
2024-05-13 00:14:45,000 [root] DEBUG: No analysis package specified, trying to detect it automagically.
2024-05-13 00:14:45,000 [root] INFO: Automatically selected analysis package "exe"
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Browser
2024-05-13 00:14:45,171 [modules.auxiliary.digisig] INFO: Skipping authenticode validation, signtool.exe was not found in bin/
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module DigiSig
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Disguise
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Human
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Screenshots
2024-05-13 00:14:45,171 [root] DEBUG: Started auxiliary module Usage
2024-05-13 00:14:45,203 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\61817e25b0cfae37a3f289fc308e67146f874342.exe" with arguments "" with pid 3064
2024-05-13 00:14:45,203 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:45,217 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 3064
192.168.56.1 - - [13/May/2024 00:14:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:46] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:14 AM


Computer
C:\Windows\system32\cmd.exe
process with pid 2320
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid
2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid
2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:03] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:05] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM


Computer
C:\Windows\system32\cmd.exe
pid: 2320
2024-05-13 00:14:53,948 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-05-13 00:14:54,137 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2320
2024-05-13 00:14:54,309 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [13/May/2024 00:14:54] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:54,355 [root] INFO: Added new process to list with pid: 2320
2024-05-13 00:14:54,355 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2320.
2024-05-13 00:14:54,684 [root] INFO: Process with pid 3064 has terminated
192.168.56.1 - - [13/May/2024 00:14:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:14:57] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:57,839 [root] INFO: Notified of termination of process with pid
2320.
2024-05-13 00:14:57,980 [root] INFO: Notified of termination of process with pid
2168.
192.168.56.1 - - [13/May/2024 00:14:58] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:58,762 [root] INFO: Process with pid 2168 has terminated
192.168.56.1 - - [13/May/2024 00:14:59] "POST /RPC2 HTTP/1.1" 200 -
2024-05-13 00:14:59,809 [root] INFO: Process with pid 2320 has terminated
192.168.56.1 - - [13/May/2024 00:15:00] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [13/May/2024 00:15:02] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
12:15 AM