VALKYRIE COMODO

Summary

File Name: virussign.com_9c564e6b5fa45c3f3460f12bb1d6baa2.exe

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

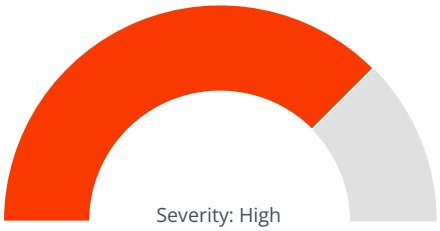
SHA1: fb359e96741bb5ccee50e40f01e64f56ae4963df

MD5: 9c564e6b5fa45c3f3460f12bb1d6baa2

MALWARE

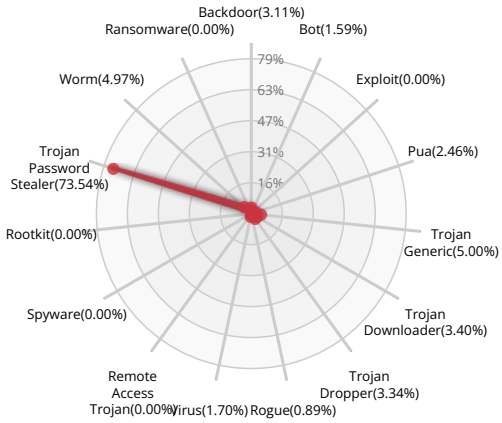
Valkyrie Final Verdict

DETECTION SECTION

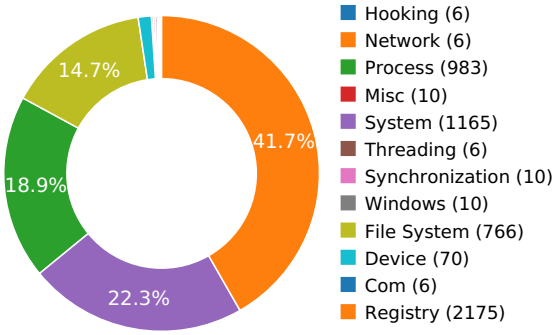


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Expresses interest in specific running processes — Show sources

Repeatedly searches for a not-found process, may want to run with startbrowser=1 option

STATIC ANOMALY

Anomalous binary characteristics — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup — Show sources

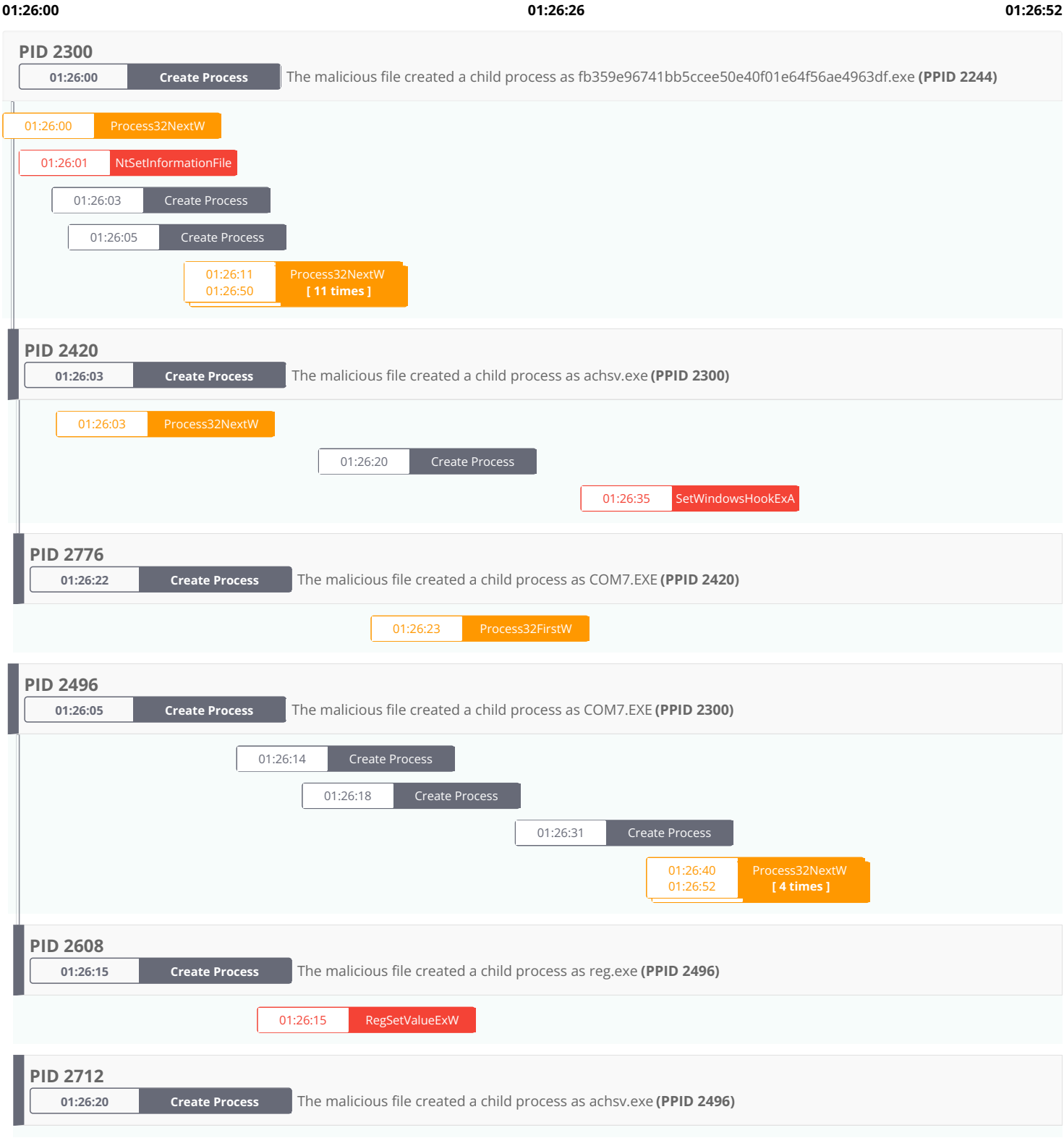
MALWARE ANALYSIS SYSTEM EVASION

Creates a hidden or system file — Show sources

STEALING OF SENSITIVE INFORMATION

Sniffs keystrokes — Show sources

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\fb359e96741bb5ccee50e40f01e64f56ae4963df.exe
C:\Windows\System32\tzres.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
\Device\KsecDD
C:\Windows\SysWOW64\shell32.dll
C:\
C:\Users
C:\Users\user\AppData\Local\Microsoft\Windows\Caches
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004f.db
C:\Users\desktop.ini
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
\??\MountPointManager
C:\Users\user\Desktop\desktop.ini
C:\Windows\System32\syssh32.dll
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\
C:
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777

\\.\C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\achsv.exe
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\achsv.exe
\\.\C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\pipe.Exc777.tmp
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\vmcis.exe
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\vmcis.txt
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PDF FoxitReader.exe
D:\
\\.\D:\Program Files\FoxitReader\bin\
\\.\
\\.\D:
\\.\D:\Program Files
\\.\D:\Program Files\FoxitReader
\\.\D:\Program Files\FoxitReader\bin
D:\Program Files\FoxitReader\bin\COM7.EXE
C:\Windows\SysWOW64\ieframe.dll
C:\REG.*
C:\Windows\System32\REG.*
C:\Windows
C:\Windows\System32
C:\Windows\SysWOW64\reg.exe
C:\Windows\SysWOW64\propsys.dll
C:\Windows\sysnative\propsys.dll
C:\Windows\System32\reg.exe
C:\Windows\System32\reg.exe:Zone.Identifier
D:\Program Files\FoxitReader\FoxitReader.exe
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\ParentFolder

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\InitFolderHandler
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
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_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\DontShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellState
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWebView
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\ClassicShell
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\SeparateProcess
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoNetCrawling
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSimpleStartMenu
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowCompColor
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DontPrettyPath

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowInfoTip
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideIcons
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\MapNetDrvBtn
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\WebView
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Filter
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\SeparateProcess
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\NoNetCrawling
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AutoCheckSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\IconsOnly
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowTypeOverlay

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\achsv.exe
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\pipe.Exc777.tmp
D:\Program Files\FoxitReader\bin\COM7.EXE
D:\Program Files\FoxitReader\FoxitReader.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PDF FoxitReader.exe

RESOLVED APIS

kernel32.dll.CreateToolhelp32Snapshot
ole32.dll.StringFromGUID2
advapi32.dll.OpenThreadToken
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
ole32.dll.CoInitializeEx
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
ole32.dll.CreateBindCtx
ole32.dll.CoTaskMemAlloc
ole32.dll.CoGetApartmentType
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoTaskMemFree
comctl32.dll.#236

oleaut32.dll.#6
ole32.dll.CoGetMalloc
comctl32.dll.#320
comctl32.dll.#324
comctl32.dll.#323
comctl32.dll.#328
comctl32.dll.#334
advapi32.dll.RegEnumKeyW
oleaut32.dll.#2
ole32.dll.CoCreateInstance
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
advapi32.dll.InitializeSecurityDescriptor
advapi32.dll.SetEntriesInAclW
ntmarta.dll.GetMartaExtensionInterface
advapi32.dll.SetSecurityDescriptorDacl
advapi32.dll.IsTextUnicode
comctl32.dll.#332
comctl32.dll.#338
comctl32.dll.#339
setupapi.dll.CM_Get_Device_Interface_List_ExW
shell32.dll.#102
comctl32.dll.#386
ole32.dll.CoUninitialize
ole32.dll.CoRevokeInitializeSpy
comctl32.dll.#388
ole32.dll.NdrOleInitializeExtension
ole32.dll.CoGetClassObject
ole32.dll.CoGetMarshalSizeMax
ole32.dll.CoMarshalInterface
ole32.dll.CoUnmarshalInterface
ole32.dll.StringFromIID
ole32.dll.CoGetPSClsid
ole32.dll.CoReleaseMarshalData
ole32.dll.DcomChannelSetHResult
oleaut32.dll.#500

advapi32.dll.RegSetValueExA
gdi32.dll.GetLayout
gdi32.dll.GdiRealizationInfo
gdi32.dll.FontIsLinked
advapi32.dll.RegOpenKeyExW
advapi32.dll.RegQueryInfoKeyW
gdi32.dll.GetTextFaceAliasW
advapi32.dll.RegEnumValueW
advapi32.dll.RegCloseKey
advapi32.dll.RegQueryValueExW
gdi32.dll.GetFontAssocStatus
advapi32.dll.RegQueryValueExA
advapi32.dll.RegEnumKeyExW
dwmapi.dll.DwmIsCompositionEnabled
gdi32.dll.GdiIsMetaPrintDC
user32.dll.GetWindowTextA
user32.dll.GetForegroundWindow
ole32.dll.OleInitialize
propsys.dll.PSCreateMemoryPropertyStore
propsys.dll.PSPropertyBag_WriteDWORD
propsys.dll.PSPropertyBag_ReadDWORD
propsys.dll.PSPropertyBag_ReadGUID
apphelp.dll.ApphelpCheckShellObject
urlmon.dll.CreateUri
kernel32.dll.InitializeSRWLock
kernel32.dll.AcquireSRWLockExclusive

DELETED REGISTRY KEYS

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

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\ParentFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Roamable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\PreCreate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Stream
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\PublishExpandedPath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\FolderTypeID
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\InitFolderHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{B97D20BB-F46A-4C97-BA10-5E3608430854}\PropertyBag

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\KnownFolders
HKEY_CURRENT_USER
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup
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\Explorer\KnownFolderSettings
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\fb359e96741bb5ccee50e40f01e64f56ae4963df.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_CLASSES_ROOT\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\Attributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\CallForAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\RestrictedAttributes
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORDISPLAY
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideFolderVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\UseDropHandler
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsFORPARSING
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsParseDisplayName
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForOverlay
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\MapNetDriveVerbs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\QueryForInfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideInWebView

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HideOnDesktopPerUser
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsAliasedNotifications
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\WantsUniversalDelegate
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\NoFileFolderJunction
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\PinToNameSpaceTree
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Wow6432Node\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder\HasNavigationEnum
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\ShellFolder
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\NonEnum\{20D04FE0-3AEA-1069-A2D8-08002B30309D}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
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_CLASSES_ROOT\Drive\shellex\FolderExtensions

EXECUTED COMMANDS

\\.\C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\achsv.exe
\\.\C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\vmcis.exe /stext "C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\vmcis.txt"
"C:\Windows\System32\reg.exe" ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /f /t REG_SZ /v COMLOADER /d "\\.\D:\Program Files\FoxitReader\bin\COM7.EXE"
REG ADD HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /f /t REG_SZ /v COMLOADER /d "\\.\D:\Program Files\FoxitReader\bin\COM7.EXE"
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\ornWllSx.exe

READ FILES

C:\Windows\System32\tzres.dll
C:\Windows\Globalization\Sorting\sortdefault.nls
\Device\KsecDD
C:\Windows\SysWOW64\shell32.dll
C:\
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004f.db
C:\Users\desktop.ini

C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
C:\Users\user\Desktop\desktop.ini
C:\Windows\System32\syssh32.dll
C:\Users\user\AppData\Local\Temp\fb359e96741bb5ccee50e40f01e64f56ae4963df.exe
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\achsv.exe
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\pipe.Exc777.tmp
C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\vmcis.txt
D:\Program Files\FoxitReader\bin\COM7.EXE
C:\Windows\SysWOW64\ieframe.dll
C:\Windows
C:\Windows\System32
D:\Program Files\FoxitReader\FoxitReader.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PDF FoxitReader.exe
C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui

MUTEXES

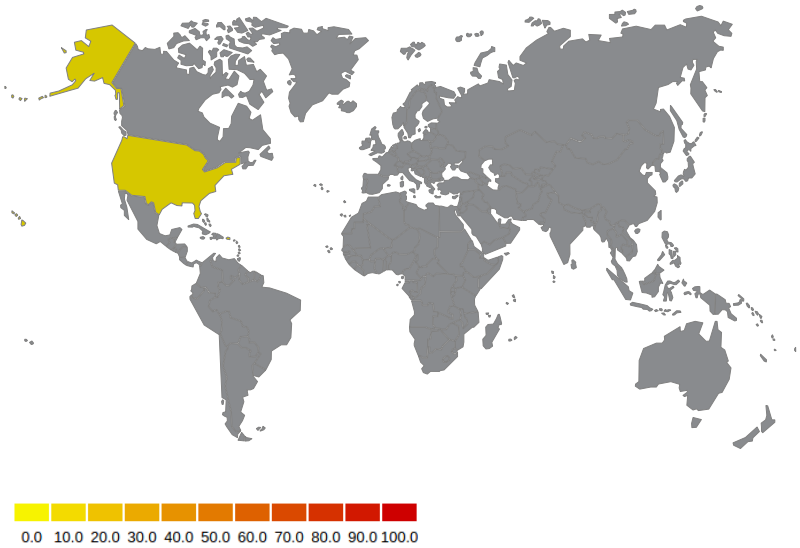
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesLockedCacheCounterMutex

MODIFIED REGISTRY KEYS

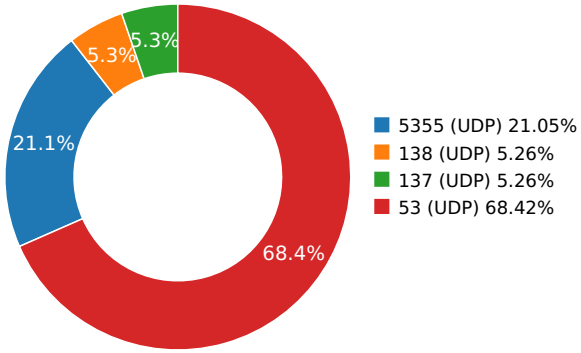
HKEY_CURRENT_USER\Software\Microsoft\winsvh
HKEY_CURRENT_USER\Software\Microsoft\winsvh\winsvh
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\COMLOADER

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
www.ibayme.eb2a.com	199.59.243.227	United States	16509	Bodis, LLC	Malware Process
www.aieov.com	45.33.30.197	United States	63949	Akamai Technologies, Inc.	Malware Process
					Malware Process
www.msftncsi.com	23.200.3.27	United States	20940	Akamai Technologies, Inc.	Malware Process

DNS QUERIES

Request	Type
5isohu.com	A
www.msftncsi.com	A
www.aieov.com	A
www.ibayme.eb2a.com	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.71524786949	Sandbox	224.0.0.252	5355
6.71796894073	Sandbox	224.0.0.252	5355
6.78439497948	Sandbox	192.168.56.255	137
8.75891184807	Sandbox	224.0.0.252	5355
9.28755784035	Sandbox	224.0.0.252	5355
10.5045039654	Sandbox	8.8.4.4	53
11.3159639835	Sandbox	8.8.4.4	53
11.5021569729	Sandbox	8.8.8.8	53
12.3152899742	Sandbox	8.8.8.8	53
12.8008139133	Sandbox	192.168.56.255	138
25.0025699139	Sandbox	8.8.8.8	53
25.3620388508	Sandbox	8.8.8.8	53
26.0023229122	Sandbox	8.8.4.4	53
26.3617370129	Sandbox	8.8.4.4	53
26.6294879913	Sandbox	8.8.8.8	53
27.6274449825	Sandbox	8.8.4.4	53
39.4152178764	Sandbox	8.8.8.8	53
40.4086768627	Sandbox	8.8.4.4	53
57.7177658081	Sandbox	8.8.8.8	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Rar$EX7.Src777\Achsv.Exe	**Type :** PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** 7f530b8cc0139cc83b39aaf6a7df15ac **SHA-1 :** 71ef339c7d075c172ea13c2dc0b1da6c0e73086e **SHA-256 :** 03f48b16b372bb029b759474349e2d0e587e690 **SHA-512 :** 12736668c292fbdba16d89e98b30a1f072d66f82 **Size :** 97.341 Kilobytes.
D:\Program Files\FoxitReader\FoxitReader.Exe	**Type :** PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** e7449b76459b7abcdd5e944a4962361d **SHA-1 :** 5e162f0df79789498e69aeae0f48220fc314dcf0 **SHA-256 :** 73e39a2b3ff5781092174590dc0256303354c6a2 **SHA-512 :** adf35c26ec6f1ac7528892f2b90365364cf8b62eft **Size :** 97.88 Kilobytes.
C:\Users\User\AppData\Local\Temp\Rar$EX7.Src777\Pipe.Exc777.Tmp	**Type :** ASCII text, with no line terminators **MD5 :** 17ee51f895f25f9b96d861b855478bf5 **SHA-1 :** f9fa24ad1803d9ae75cccc56b89af04adec56225 **SHA-256 :** 50f040cd185ddb0137bc028a5d969f1c1c67c6cfa **SHA-512 :** 83b744ffbbf8101d8c964b8d74a443dab9950188 **Size :** 0.01 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PDF FoxitReader.Exe	**Type :** PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** a7e03d4ac195381df91875cfcc054565 **SHA-1 :** c47b33ace0f73d20dd622c19f0e55a1a4ab781ae **SHA-256 :** 7606ed32c65364f5094cb36fe990065094e24813 **SHA-512 :** 44ba8e69e826ed2aba7b53a1ebf268525dfc715a **Size :** 97.613 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	virussign.com_9c564e6b5fa45c3f3460f12bb1d6baa2.exe
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
SHA1:	fb359e96741bb5ccee50e40f01e64f56ae4963df
MD5:	9c564e6b5fa45c3f3460f12bb1d6baa2
First Seen Date:	2025-01-01 00:56:51.458166 (about 4 hours ago)
Number Of Clients Seen:	2
Last Analysis Date:	2025-01-01 00:56:51.458166 (about 4 hours ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

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	8
Trid	[[42.6, u'Win32 Executable (generic)'], [19.1, u'OS/2 Executable (generic)'], [18.9, u'Generic Win/DOS Executable'], [18.9, u'DOS Executable Generic'], [0.2, u'VXD Driver']]
Compilation Time Stamp	0x501FE276 [Mon Aug 6 15:27:50 2012 UTC]
ProductVersion	1.10
InternalName	PDFReader
FileVersion	1.10
OriginalFilename	PDFReader.exe
ProductName	PDF_Reader_1.1
Translation	0x0409 0x04b0
Entry Point	0x401240 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	97130
Ssdeep	1536:VUMTIGU8vM3dG7l5rphVgEQF5NM4Jt78eRL2h+nhMJ41mxZhYFR6:VbTIGbvM3dIhVYFU4JtVRqYnCJ41mrhD
Sha256	caa42554c17fd53b04b0f98a6e57f0f67ada0fae2364e4a58de5c9543b9eae4f
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/f/b/3/5/fb359e96741bb5ccee50e40f01e64f56ae4963df', u'EXE:OriginalFileName': u'PDFReader.exe', u'EXE:ProductName': u'PDF_Reader_1.1', u'EXE:InternalName': u'PDFReader', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2025:01:01 00:56:41+00:00', u'EXE:InitializedDataSize': 72704, u'File:FileModifyDate': u'2025:01:01 00:56:29+00:00', u'EXE:FileVersionNumber': u'1.1.0.0', u'EXE:FileVersion': 1.1, u'File:FileSize': u'95 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': 1.1, u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 1263616, u'File:FileName': u'fb359e96741bb5ccee50e40f01e64f56ae4963df', u'EXE:ImageVersion': 1.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2012:08:06 15:27:50+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LinkerVersion': 2.56, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/f/b/3/5', u'EXE:EntryPoint': u'0x1240', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 28160, u'File:FileInodeChangeDate': u'2025:01:01 00:56:40+00:00', u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.1.0.0'}]
Mime Type	application/x-dosexec
Imphash	ea28f662ab831803e9a8c823439760d0

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6df4	0x6e00	5.71637695075	4818edbbf49e728d29da60ab09a44c12
.data	0x8000	0x14e0	0x1600	3.58044041631	9aaaacb788efde655842192c957defc6
.rdata	0xa000	0x1440	0x1600	4.48186586391	4594b8be00878509965f238fa77d0baa
.bss	0xc000	0x1346e0	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.edata	0x141000	0x44	0x200	0.733238891114	630f0d1996612d2971af0f4441212f53
.idata	0x142000	0xbdc	0xc00	4.87090107266	c4fa261f310a3283820f0e89192ad762
.reloc	0x143000	0x5a4	0x600	6.4362570655	815dfc593a4ebc0a4b4dd0d9c6af708a
.rsrc	0x144000	0x6c60	0x6e00	5.07077100032	57a728889cf64fb09607acb49d19b92a

PE Imports

- msvcrt.dll
  - _getcwd
  - _mkdir
  - _sleep
  - _stat
  - _strlwr
- msvcrt.dll
  - __getmainargs
  - __p__environ
  - __p__fmode
  - __set_app_type
  - _cexit
  - _errno
  - _findclose
  - _findfirst
  - _findnext
  - _fullpath
  - _iob
  - _onexit
  - _setmode
  - abort
  - atexit
  - difftime
  - exit
  - fclose
  - fflush
  - fopen
  - fprintf
  - fputc
  - fread
  - free
  - fseek
  - fwrite
  - getenv
  - localtime
  - malloc
  - printf
  - rand
  - signal
  - srand
  - time
- ADVAPI32.DLL
  - RegCloseKey
  - RegCreateKeyExA
  - RegOpenKeyExA
  - RegQueryValueExA
- KERNEL32.dll
  - AddAtomA
  - CloseHandle
  - CreateProcessA
  - CreateThread
  - CreateToolhelp32Snapshot
  - ExitProcess
  - FindAtomA

- GetAtomNameA
- GetDriveTypeA
- GetFileAttributesA
- GetLastError
- GetLogicalDriveStringsA
- GetModuleHandleA
- GetProcAddress
- LoadLibraryA
- Module32First
- Process32First
- Process32Next
- SetFileAttributesA
- SetUnhandledExceptionFilter

- ntdll.dll
  - atoi
  - atol
  - memcpy
  - memset
  - sprintf
  - strcat
  - strcpy
  - strlen
  - tolower
- SHELL32.DLL
  - SHGetPathFromIDListA
  - SHGetSpecialFolderLocation
  - ShellExecuteA
- USER32.dll
  - CallNextHookEx
  - DispatchMessageA
  - GetKeyNameTextA
  - GetMessageA
  - MessageBoxA
  - SetWindowsHookExA
  - TranslateMessage
  - UnhookWindowsHookEx
- WS2_32.DLL
  - WSACleanup
  - WSAStartup
  - __WSAFDIsSet
  - accept
  - bind
  - closesocket
  - connect
  - getaddrinfo
  - gethostbyname
  - gethostname
  - htons
  - listen
  - recv
  - select
  - send
  - socket

PE Exports

CeyEvent@12

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1327672, u'sha256': u'e0c351507075358eff3e3f59cccc6ffc05d9457c28ec7290d95a6a8152f7987f', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1329056, u'sha256': u'601795e94fd4baef74f20a093a028025dfe7ef48a692e21eafd15b6df95f0119', u'type': u'data', u'size': 1736}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1330792, u'sha256': u'22b9b3c2563e5ca387b6fb3ecb36cc9bb986a8bf93b9096ae01224b024843006', u'type': u'dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 15724785, next used block 15726591', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1333008, u'sha256': u'bf57adf04fcf9288ee0127cc3e1f4c13ec5571df98b277c790b8b534ef28cf3d', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1336760, u'sha256': u'e948e2f712eca39f7e6bef7114b36d9421afd769377a46d318d5cbf37ad353f2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1337888, u'sha256': u'453b6c32996619ba78cd53b419fcf32f7c5fc6715bf57dfaa7df792196ec28c6', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1340328, u'sha256':

u'f57854486eef3671d59e5cf4c6066ef4fd11cd4278467b662e1673b1b6a7b3f4', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 1344592, u'sha256': u'f88a10f632cfce380b89b66dab5f16381010a9e64df6429e8a07a9a8cf016b5d', u'type': u'data', u'size': 9640}

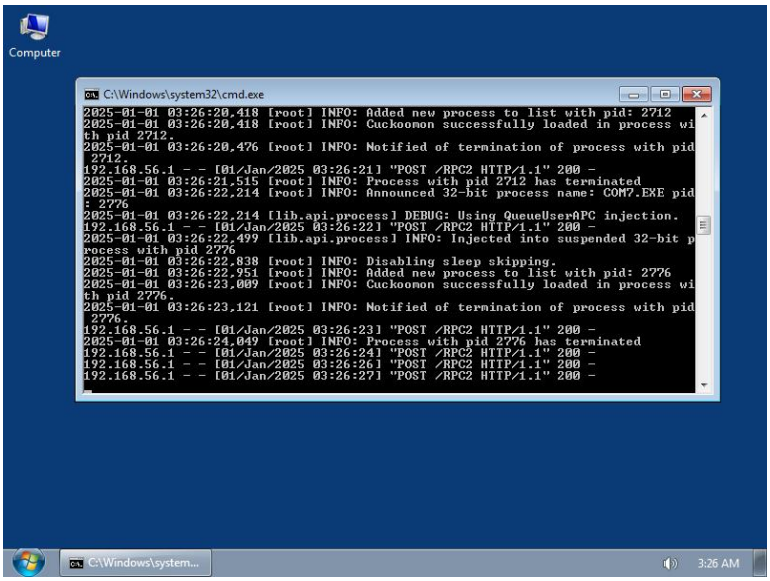
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 1354232, u'sha256': u'03a2f5f19b878f738c442e8e2e89dcc416e0ba0380590534cfa2cb39dd8bb51d', u'type': u'MS Windows icon resource - 8 icons, 16x16', u'size': 118}

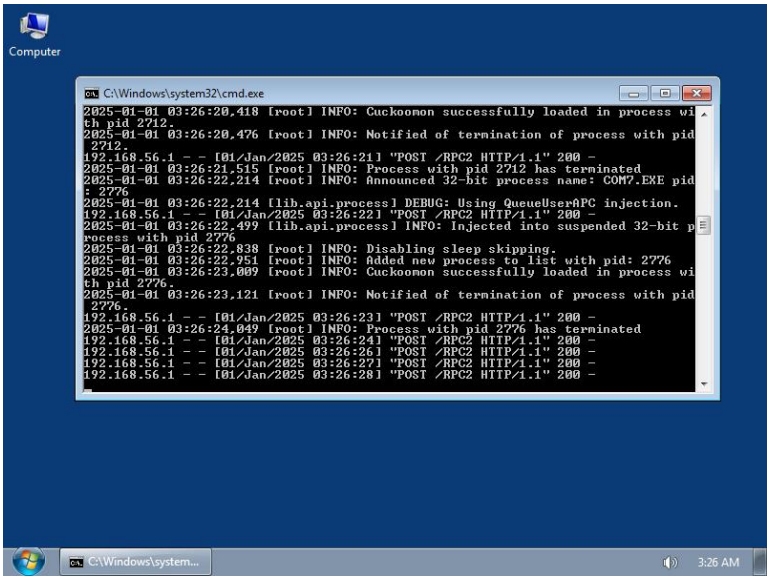
{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 1354352, u'sha256': u'e4ee5b17d2733412c32f159522b52d4de91cd99ac687c793740da8a2ee4dbc6a', u'type': u'MS Windows COFF PowerPC object file', u'size': 496}

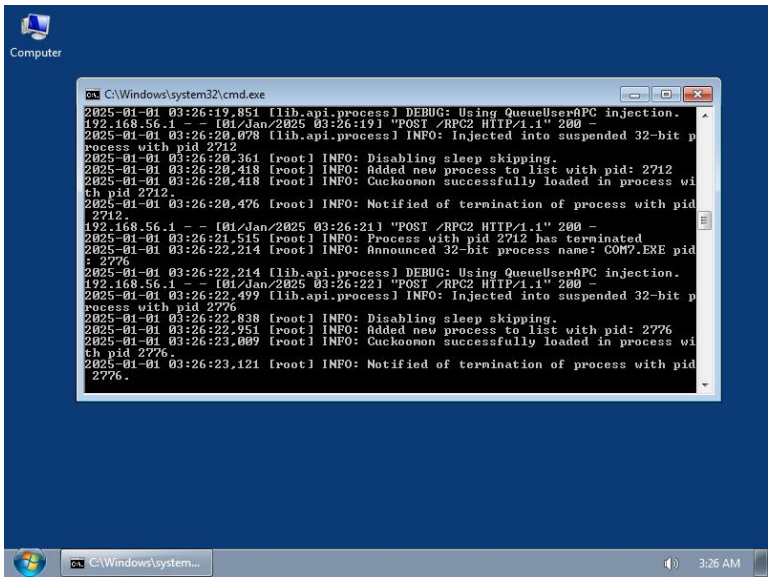
CERTIFICATE VALIDATION

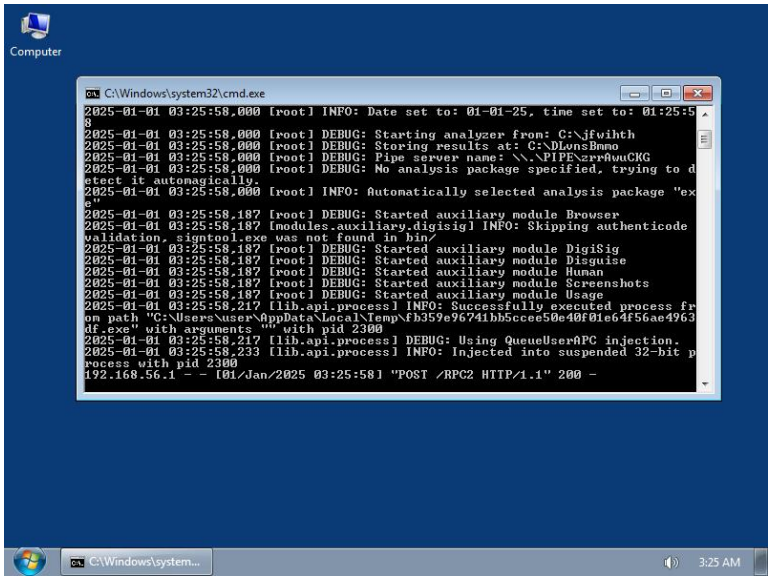
- Certificate Validation is not Applicable ?

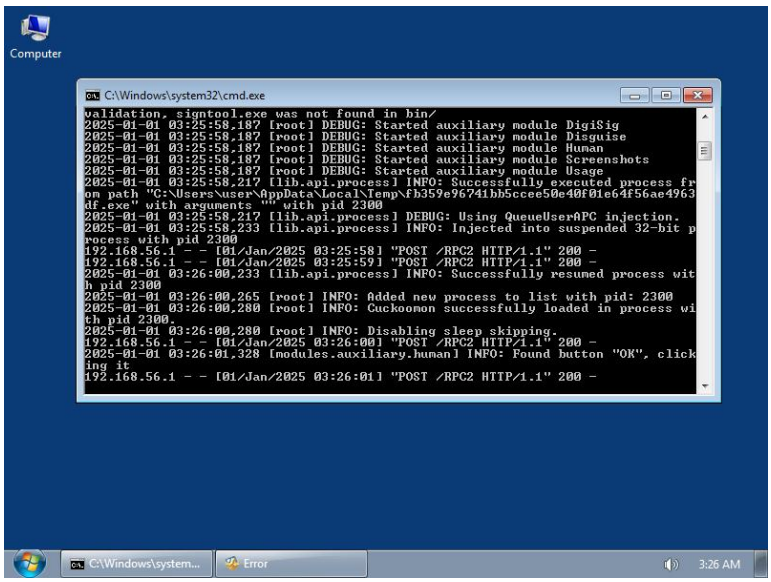
SCREENSHOTS

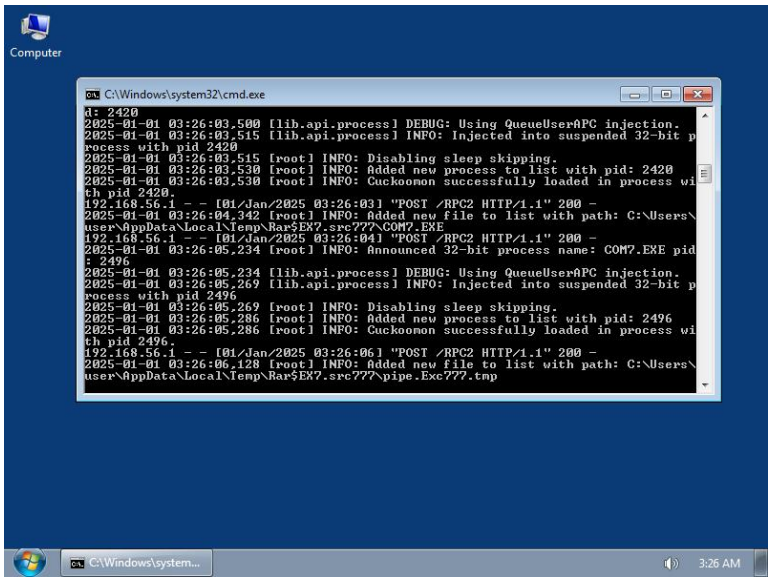


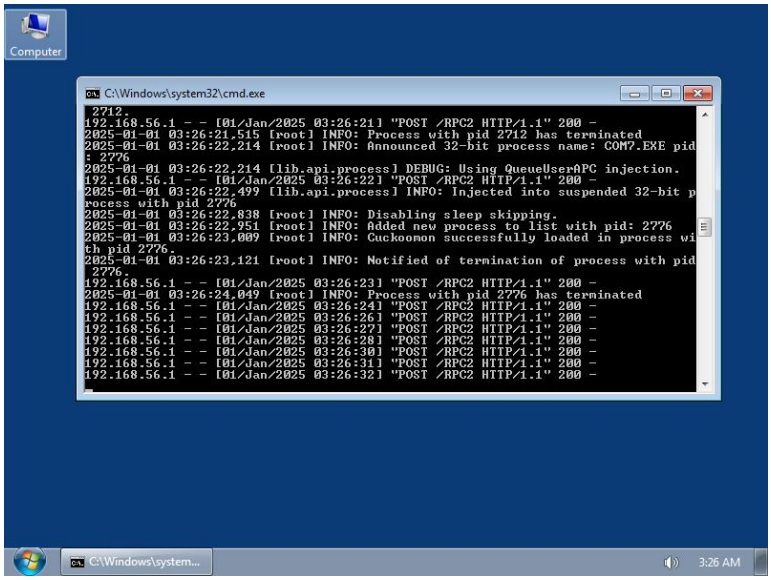


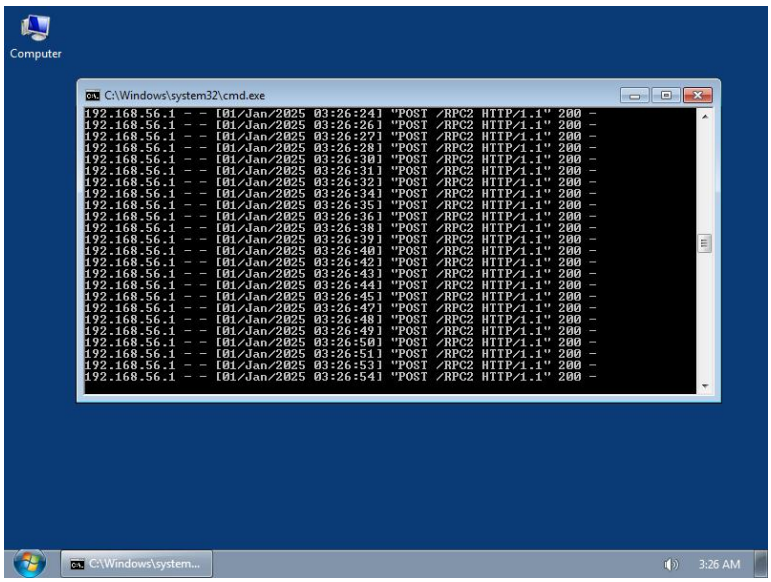

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:19,851 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:19] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:20,078 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2712
2025-01-01 03:26:20,361 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:20,418 [root] INFO: Added new process to list with pid: 2712
2025-01-01 03:26:20,418 [root] INFO: Cuckoomon successfully loaded in process with pid 2712.
2025-01-01 03:26:20,476 [root] INFO: Notified of termination of process with pid 2712.
192.168.56.1 - - [01/Jan/2025 03:26:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:21,515 [root] INFO: Process with pid 2712 has terminated
2025-01-01 03:26:22,214 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2776
2025-01-01 03:26:22,214 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process with pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid 2776.
C:\Windows\system...
3:26 AM

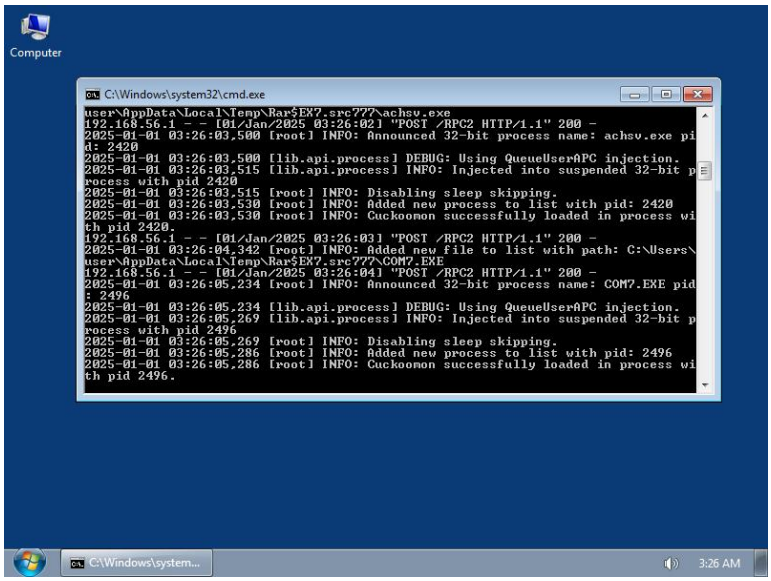

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:25:58,000 [root] INFO: Date set to: 01-01-25, time set to: 01:25:58
2025-01-01 03:25:58,000 [root] DEBUG: Starting analyzer from: C:\jfwihth
2025-01-01 03:25:58,000 [root] DEBUG: Storing results at: C:\DLvnsBmmo
2025-01-01 03:25:58,000 [root] DEBUG: Pipe server name: \\.\PIPE\zrrAwuCKG
2025-01-01 03:25:58,000 [root] DEBUG: No analysis package specified, trying to detect it automagically.
2025-01-01 03:25:58,000 [root] INFO: Automatically selected analysis package "exe"
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Browser
2025-01-01 03:25:58,187 [modules.auxiliary.digisig] INFO: Skipping authenticode validation, signtool.exe was not found in bin/
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module DigiSig
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Disguise
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Human
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Screenshots
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Usage
2025-01-01 03:25:58,217 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\fb359e9674ibb5ccee50e40f01e64f56ae4963df.exe" with arguments "" with pid 2300
2025-01-01 03:25:58,217 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:25:58,233 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2300
192.168.56.1 - - [01/Jan/2025 03:25:58] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:25 AM

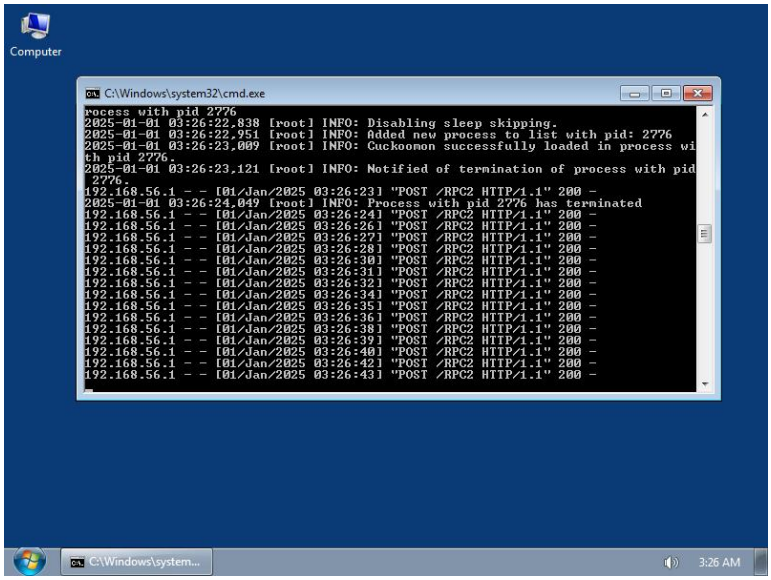

Computer
C:\Windows\system32\cmd.exe
validation, signtool.exe was not found in bin/
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module DigiSig
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Disguise
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Human
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Screenshots
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Usage
2025-01-01 03:25:58,217 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\fb359e9674ibb5ccee50e40f01e64f56ae4963df.exe" with arguments "" with pid 2300
2025-01-01 03:25:58,217 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:25:58,233 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2300
192.168.56.1 - - [01/Jan/2025 03:25:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:25:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:00,233 [lib.api.process] INFO: Successfully resumed process with pid 2300
2025-01-01 03:26:00,265 [root] INFO: Added new process to list with pid: 2300
2025-01-01 03:26:00,280 [root] INFO: Cuckoomon successfully loaded in process with pid 2300.
2025-01-01 03:26:00,280 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [01/Jan/2025 03:26:00] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:01,328 [modules.auxiliary.human] INFO: Found button "OK", clicking it
192.168.56.1 - - [01/Jan/2025 03:26:01] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Error
3:26 AM

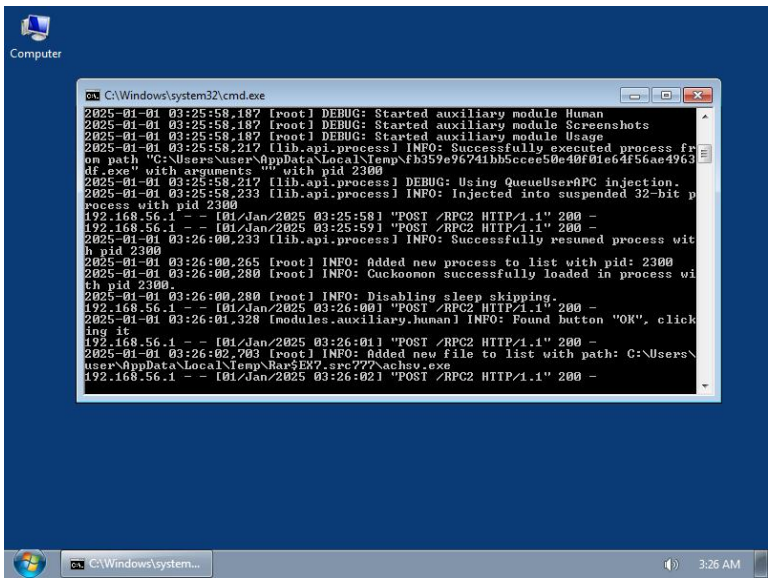

Computer
C:\Windows\system32\cmd.exe
d: 2420
2025-01-01 03:26:03,500 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:03,515 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2420
2025-01-01 03:26:03,515 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:03,530 [root] INFO: Added new process to list with pid: 2420
2025-01-01 03:26:03,530 [root] INFO: Cuckoomon successfully loaded in process with pid 2420.
192.168.56.1 - - [01/Jan/2025 03:26:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:04,342 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:04] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:05,234 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2496
2025-01-01 03:26:05,234 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:05,269 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2496
2025-01-01 03:26:05,269 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:05,286 [root] INFO: Added new process to list with pid: 2496
2025-01-01 03:26:05,286 [root] INFO: Cuckoomon successfully loaded in process with pid 2496.
192.168.56.1 - - [01/Jan/2025 03:26:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:06,128 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\pipe.Exc777.tmp
C:\Windows\system...
3:26 AM

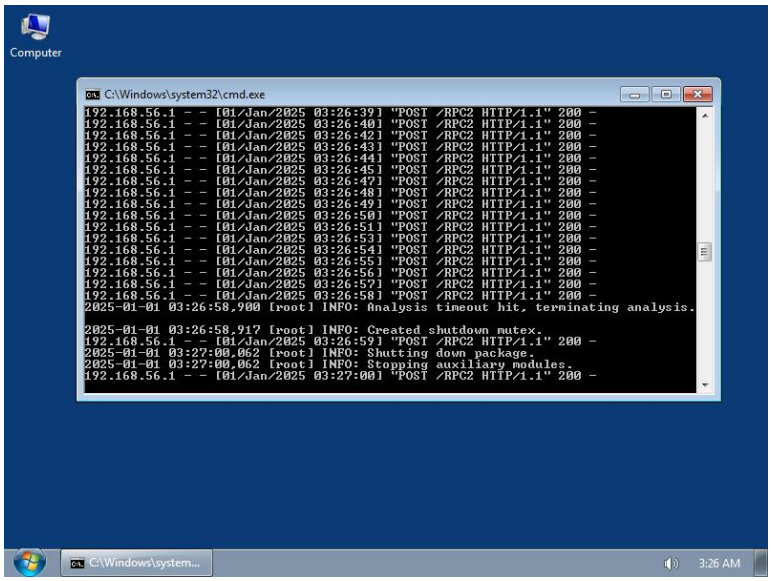

Computer
C:\Windows\system32\cmd.exe
2712.
192.168.56.1 - - [01/Jan/2025 03:26:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:21,515 [root] INFO: Process with pid 2712 has terminated
2025-01-01 03:26:22,214 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2776
2025-01-01 03:26:22,214 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process with pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid 2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

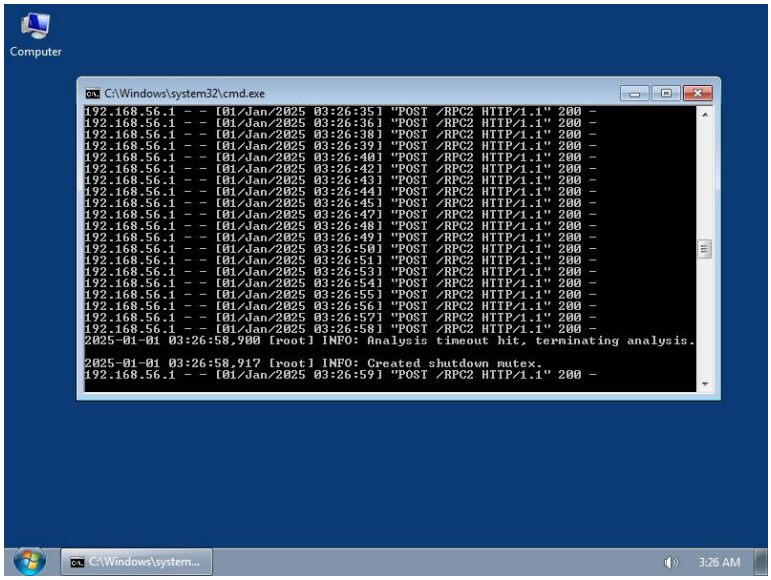

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:54] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

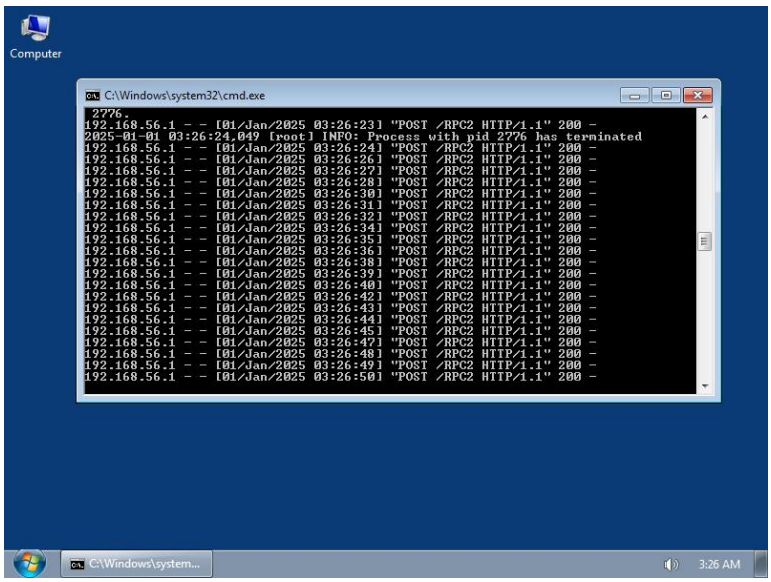

Computer
C:\Windows\system32\cmd.exe
user\AppData\Local\Temp\Rar$EX7.src777\achsv.exe
192.168.56.1 - - [01/Jan/2025 03:26:02] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:03,500 [root] INFO: Announced 32-bit process name: achsv.exe pi
d: 2420
2025-01-01 03:26:03,500 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:03,515 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2420
2025-01-01 03:26:03,515 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:03,530 [root] INFO: Added new process to list with pid: 2420
2025-01-01 03:26:03,530 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2420.
192.168.56.1 - - [01/Jan/2025 03:26:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:04,342 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:04] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:05,234 [root] INFO: Announced 32-bit process name: COM7.EXE pid
: 2496
2025-01-01 03:26:05,234 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:05,269 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2496
2025-01-01 03:26:05,269 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:05,286 [root] INFO: Added new process to list with pid: 2496
2025-01-01 03:26:05,286 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2496.
C:\Windows\system...
3:26 AM

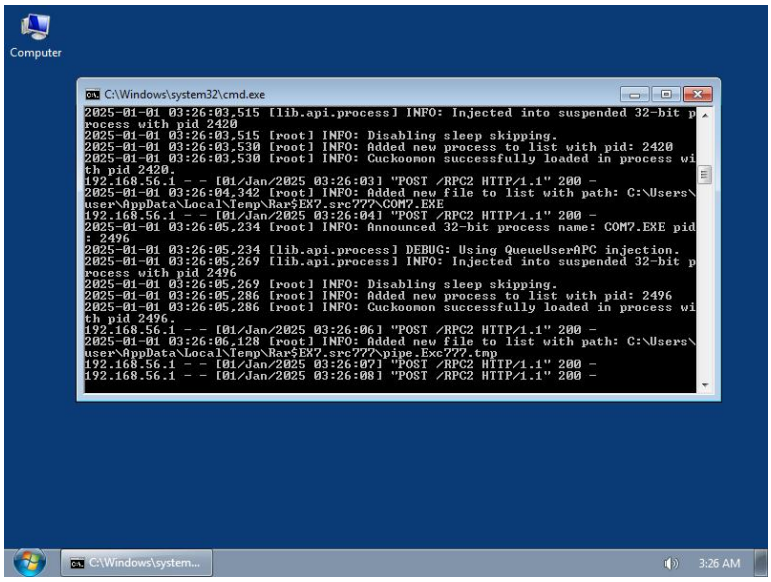

Computer
C:\Windows\system32\cmd.exe
rocess with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid
2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

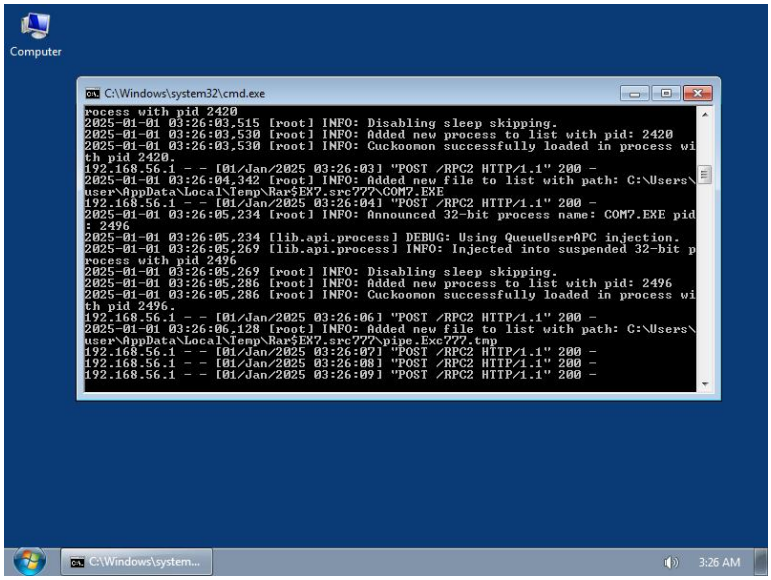

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Human
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Screenshots
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Usage
2025-01-01 03:25:58,217 [lib.api.process] INFO: Successfully executed process fr
om path "C:\Users\user\AppData\Local\Temp\fb359e96741bb5ccee50e40f01e64f56ae4963
df.exe" with arguments "" with pid 2300
2025-01-01 03:25:58,217 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:25:58,233 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2300
192.168.56.1 - - [01/Jan/2025 03:25:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:25:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:00,233 [lib.api.process] INFO: Successfully resumed process wit
h pid 2300
2025-01-01 03:26:00,265 [root] INFO: Added new process to list with pid: 2300
2025-01-01 03:26:00,280 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2300.
2025-01-01 03:26:00,280 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [01/Jan/2025 03:26:00] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:01,328 [modules.auxiliary.human] INFO: Found button "OK", click
ing it
192.168.56.1 - - [01/Jan/2025 03:26:01] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:02,703 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Rar$EX7.src777\achsv.exe
192.168.56.1 - - [01/Jan/2025 03:26:02] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

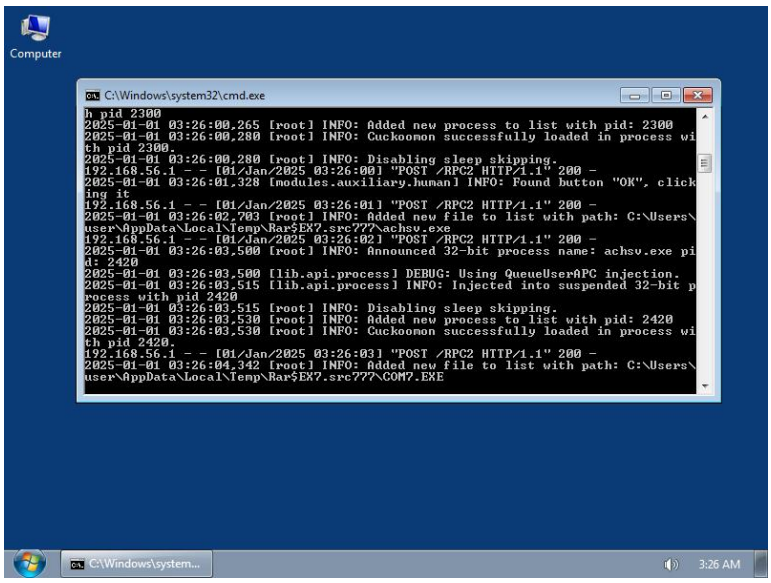

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:58,900 [root] INFO: Analysis timeout hit, terminating analysis.
2025-01-01 03:26:58,917 [root] INFO: Created shutdown mutex.
192.168.56.1 - - [01/Jan/2025 03:26:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:27:00,062 [root] INFO: Shutting down package.
2025-01-01 03:27:00,062 [root] INFO: Stopping auxiliary modules.
192.168.56.1 - - [01/Jan/2025 03:27:00] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

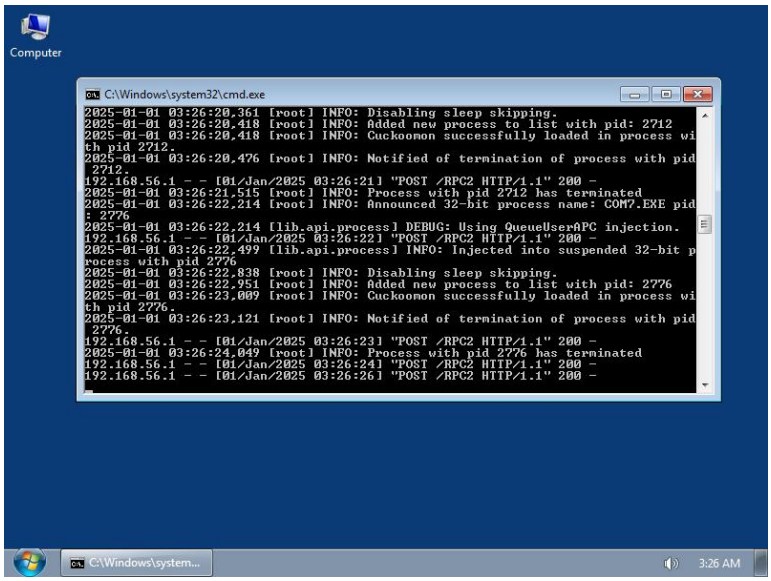

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:58] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:58,900 [root] INFO: Analysis timeout hit, terminating analysis.
2025-01-01 03:26:58,917 [root] INFO: Created shutdown mutex.
192.168.56.1 - - [01/Jan/2025 03:26:59] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

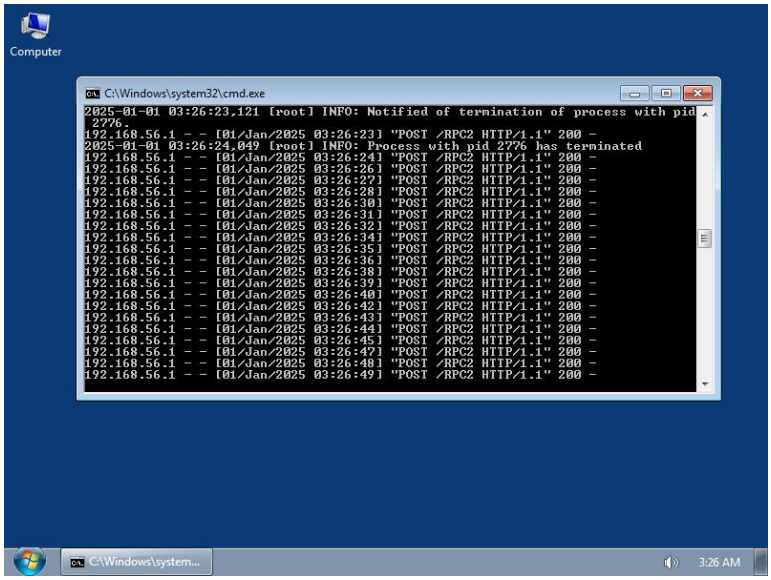

Computer
C:\Windows\system32\cmd.exe
2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:50] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

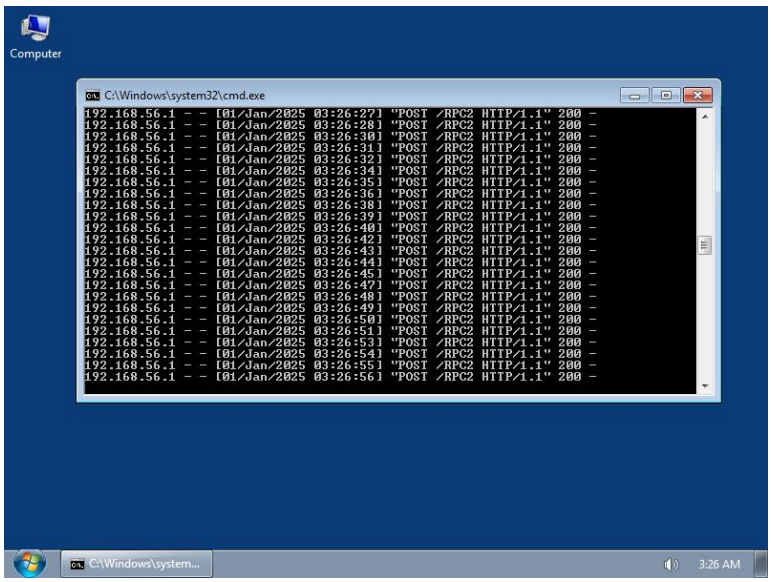

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:03,515 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2420
2025-01-01 03:26:03,515 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:03,530 [root] INFO: Added new process to list with pid: 2420
2025-01-01 03:26:03,530 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2420.
192.168.56.1 - - [01/Jan/2025 03:26:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:04,342 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:04] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:05,234 [root] INFO: Announced 32-bit process name: COM7.EXE pid
: 2496
2025-01-01 03:26:05,234 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:05,269 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2496
2025-01-01 03:26:05,269 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:05,286 [root] INFO: Added new process to list with pid: 2496
2025-01-01 03:26:05,286 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2496.
192.168.56.1 - - [01/Jan/2025 03:26:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:06,128 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Rar$EX7.src777\pipe.Exc777.tmp
192.168.56.1 - - [01/Jan/2025 03:26:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:08] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

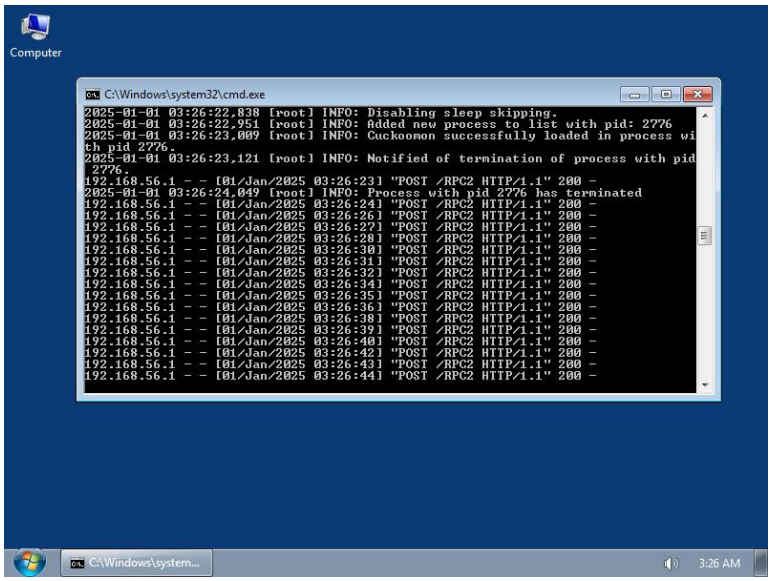

Computer
C:\Windows\system32\cmd.exe
rocess with pid 2420
2025-01-01 03:26:03,515 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:03,530 [root] INFO: Added new process to list with pid: 2420
2025-01-01 03:26:03,530 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2420.
192.168.56.1 - - [01/Jan/2025 03:26:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:04,342 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:04] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:05,234 [root] INFO: Announced 32-bit process name: COM7.EXE pid
: 2496
2025-01-01 03:26:05,234 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:05,269 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2496
2025-01-01 03:26:05,269 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:05,286 [root] INFO: Added new process to list with pid: 2496
2025-01-01 03:26:05,286 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2496.
192.168.56.1 - - [01/Jan/2025 03:26:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:06,128 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Rar$EX7.src777\pipe.Exc777.tmp
192.168.56.1 - - [01/Jan/2025 03:26:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:09] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

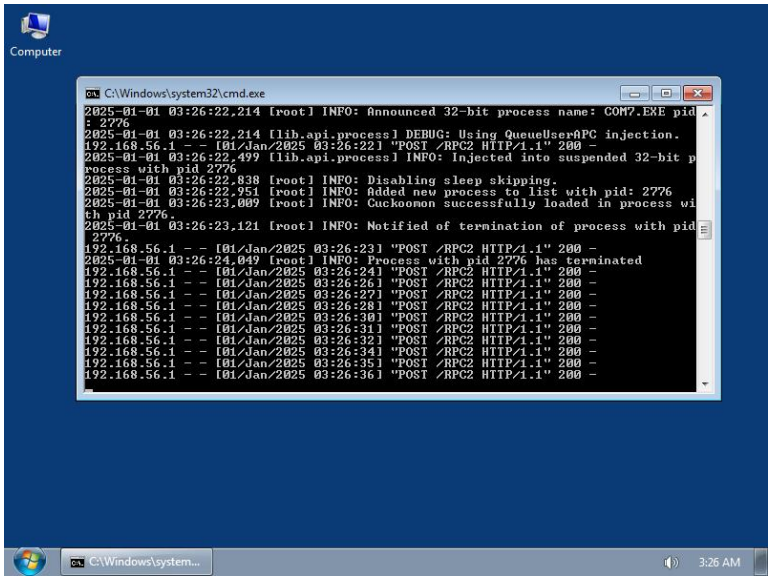

Computer
C:\Windows\system32\cmd.exe
h pid 2300
2025-01-01 03:26:00,265 [root] INFO: Added new process to list with pid: 2300
2025-01-01 03:26:00,280 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2300.
2025-01-01 03:26:00,280 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [01/Jan/2025 03:26:00] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:01,328 [modules.auxiliary.human] INFO: Found button "OK", click
ing it
192.168.56.1 - - [01/Jan/2025 03:26:01] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:02,703 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Rar$EX7.src777\achsv.exe
192.168.56.1 - - [01/Jan/2025 03:26:02] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:03,500 [root] INFO: Announced 32-bit process name: achsv.exe pi
d: 2420
2025-01-01 03:26:03,500 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:03,515 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2420
2025-01-01 03:26:03,515 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:03,530 [root] INFO: Added new process to list with pid: 2420
2025-01-01 03:26:03,530 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2420.
192.168.56.1 - - [01/Jan/2025 03:26:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:04,342 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
C:\Windows\system...
3:26 AM

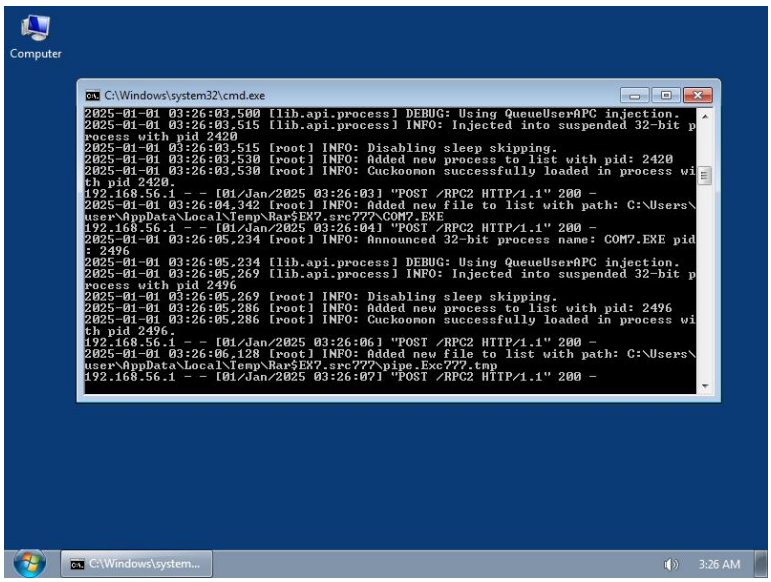

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:20,361 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:20,418 [root] INFO: Added new process to list with pid: 2712
2025-01-01 03:26:20,418 [root] INFO: Cuckoomon successfully loaded in process with pid 2712.
2025-01-01 03:26:20,476 [root] INFO: Notified of termination of process with pid 2712.
192.168.56.1 - - [01/Jan/2025 03:26:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:21,515 [root] INFO: Process with pid 2712 has terminated
2025-01-01 03:26:22,214 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2776
2025-01-01 03:26:22,214 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process with pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid 2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

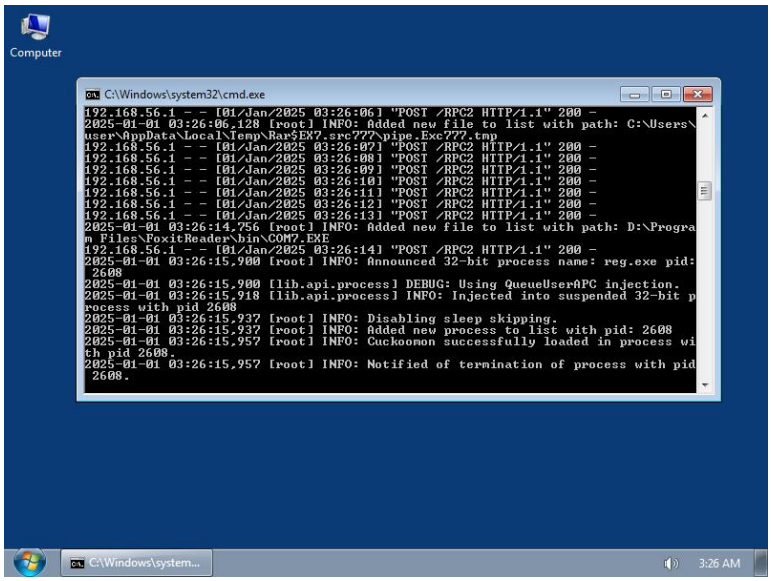

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid 2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:49] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

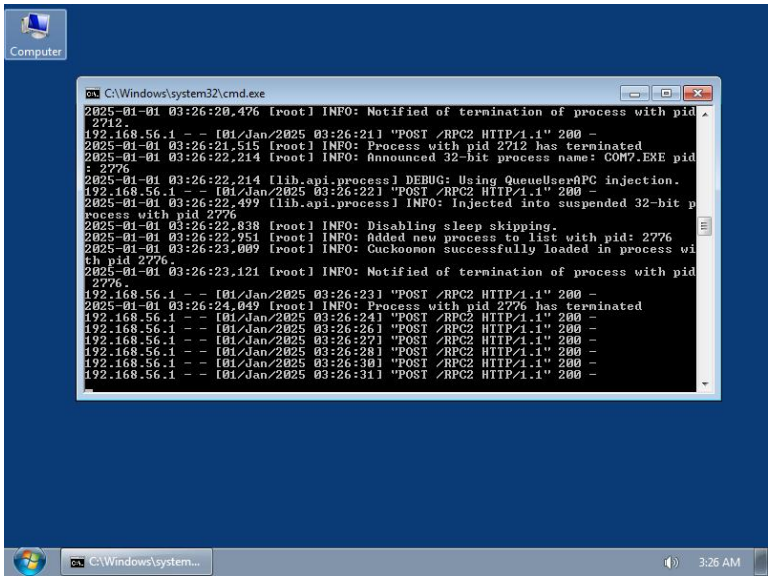

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:56] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

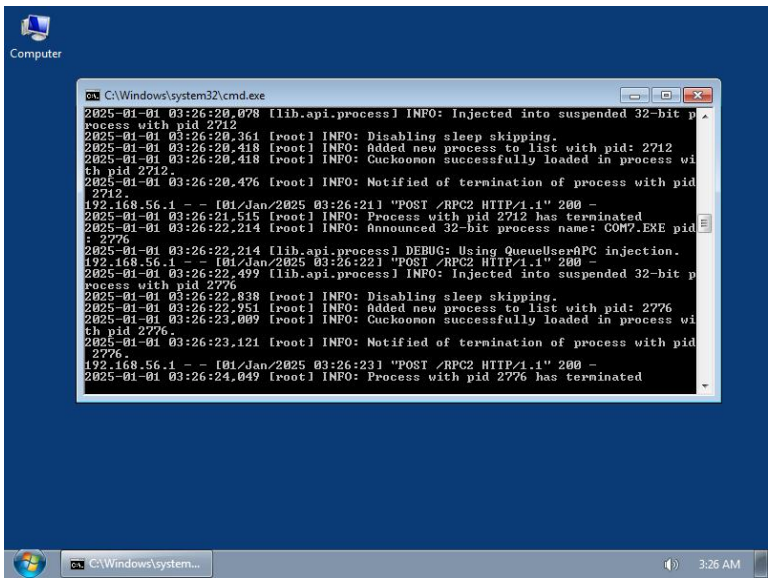

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process with pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid 2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

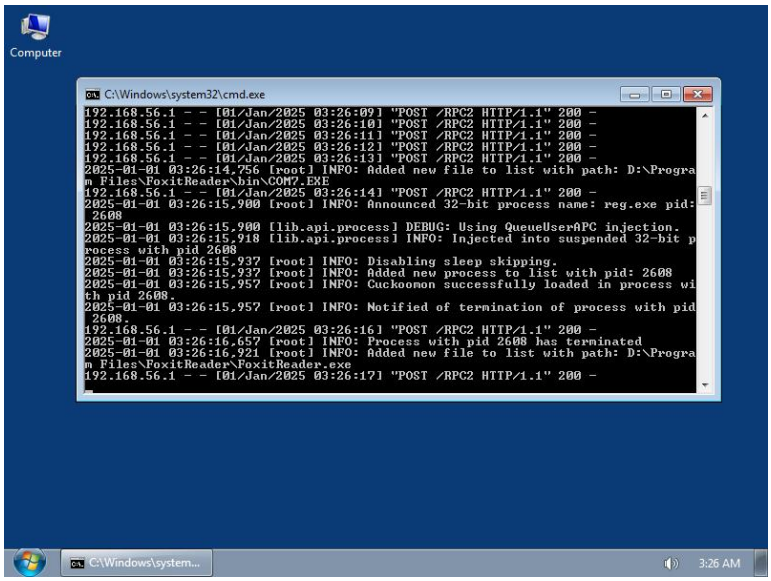

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:22,214 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2776
2025-01-01 03:26:22,214 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process with pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid 2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

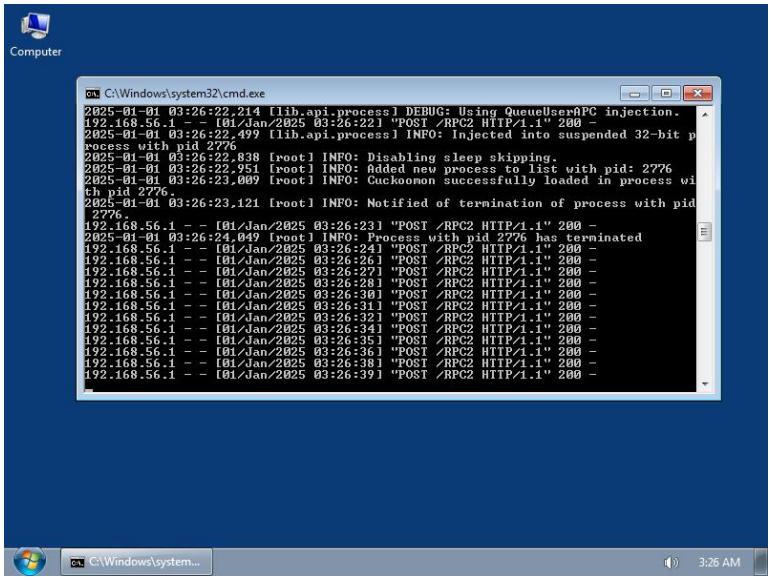

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:03,500 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:03,515 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2420
2025-01-01 03:26:03,515 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:03,530 [root] INFO: Added new process to list with pid: 2420
2025-01-01 03:26:03,530 [root] INFO: Cuckoomon successfully loaded in process with pid 2420.
192.168.56.1 - - [01/Jan/2025 03:26:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:04,342 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:04] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:05,234 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2496
2025-01-01 03:26:05,234 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:05,269 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2496
2025-01-01 03:26:05,269 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:05,286 [root] INFO: Added new process to list with pid: 2496
2025-01-01 03:26:05,286 [root] INFO: Cuckoomon successfully loaded in process with pid 2496.
192.168.56.1 - - [01/Jan/2025 03:26:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:06,128 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\pipe.Exc777.tmp
192.168.56.1 - - [01/Jan/2025 03:26:07] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

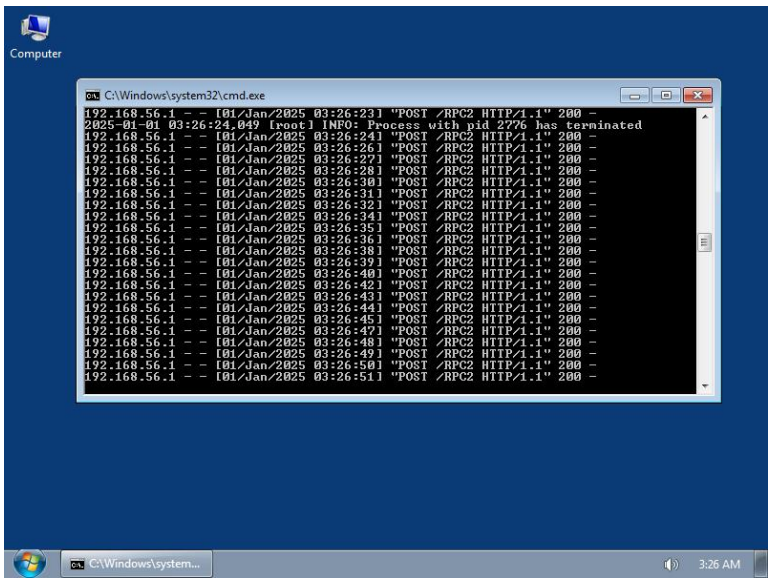

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:06,128 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Rar$EX07.src777\pips.Exe777.tmp
192.168.56.1 - - [01/Jan/2025 03:26:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:13] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:14,756 [root] INFO: Added new file to list with path: D:\Program Files\FoxitReader\bin\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:15,900 [root] INFO: Announced 32-bit process name: reg.exe pid: 2608
2025-01-01 03:26:15,900 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:15,918 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2608
2025-01-01 03:26:15,937 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:15,937 [root] INFO: Added new process to list with pid: 2608
2025-01-01 03:26:15,957 [root] INFO: Cuckoomon successfully loaded in process with pid 2608.
2025-01-01 03:26:15,957 [root] INFO: Notified of termination of process with pid 2608.
C:\Windows\system...
3:26 AM

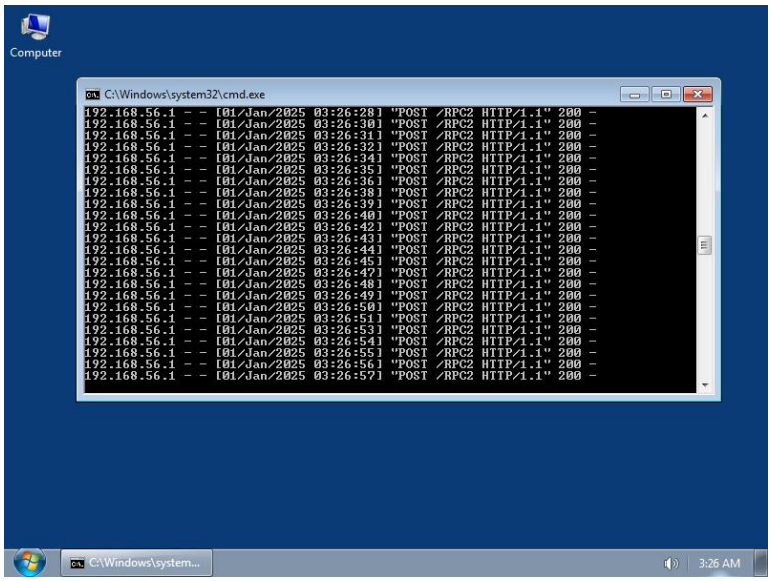

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:20,476 [root] INFO: Notified of termination of process with pid 2712.
192.168.56.1 - - [01/Jan/2025 03:26:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:21,515 [root] INFO: Process with pid 2712 has terminated
2025-01-01 03:26:22,214 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2776
2025-01-01 03:26:22,214 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process with pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid 2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

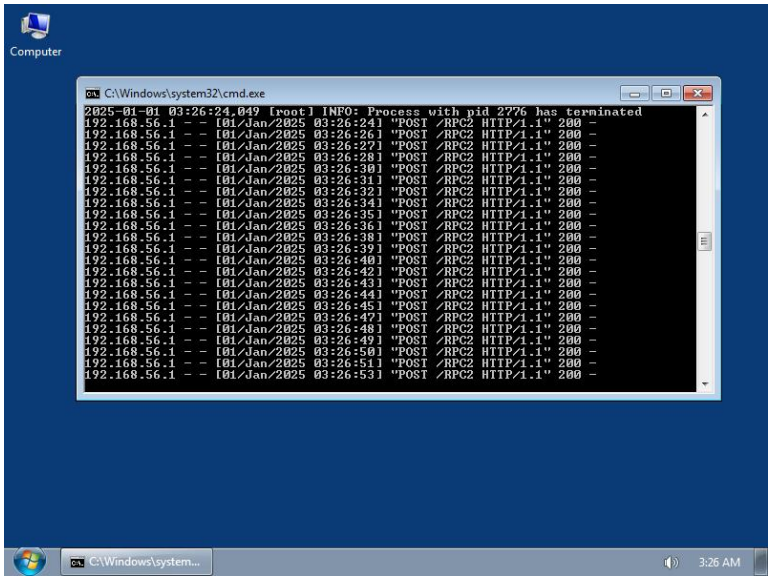

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:20,078 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2712
2025-01-01 03:26:20,361 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:20,418 [root] INFO: Added new process to list with pid: 2712
2025-01-01 03:26:20,418 [root] INFO: Cuckoomon successfully loaded in process with pid 2712.
2025-01-01 03:26:20,476 [root] INFO: Notified of termination of process with pid 2712.
192.168.56.1 - - [01/Jan/2025 03:26:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:21,515 [root] INFO: Process with pid 2712 has terminated
2025-01-01 03:26:22,214 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2776
2025-01-01 03:26:22,214 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process with pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid 2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
C:\Windows\system...
3:26 AM

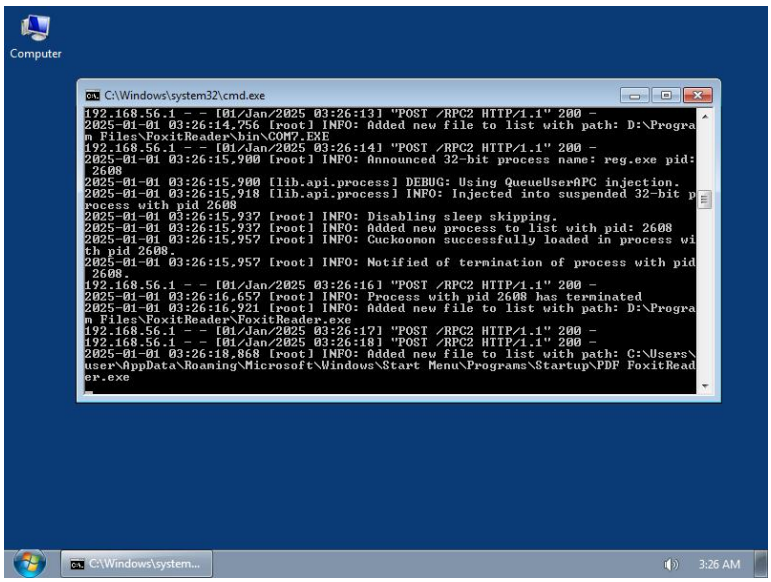

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:13] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:14,756 [root] INFO: Added new file to list with path: D:\Program Files\FoxitReader\bin\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:15,900 [root] INFO: Announced 32-bit process name: reg.exe pid: 2608
2025-01-01 03:26:15,900 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:15,918 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2608
2025-01-01 03:26:15,937 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:15,937 [root] INFO: Added new process to list with pid: 2608
2025-01-01 03:26:15,957 [root] INFO: Cuckoomon successfully loaded in process with pid 2608.
2025-01-01 03:26:15,957 [root] INFO: Notified of termination of process with pid 2608.
192.168.56.1 - - [01/Jan/2025 03:26:16] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:16,657 [root] INFO: Process with pid 2608 has terminated
2025-01-01 03:26:16,921 [root] INFO: Added new file to list with path: D:\Program Files\FoxitReader\FoxitReader.exe
192.168.56.1 - - [01/Jan/2025 03:26:17] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

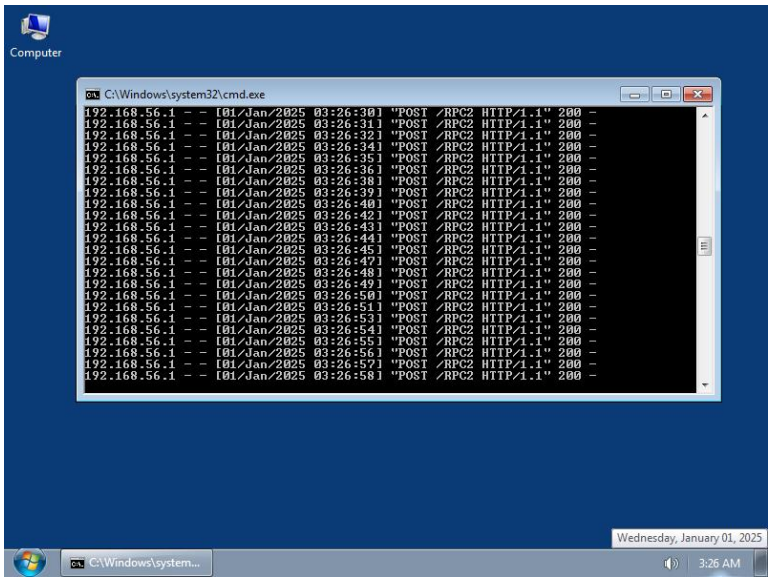

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:22,214 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process with pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid 2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

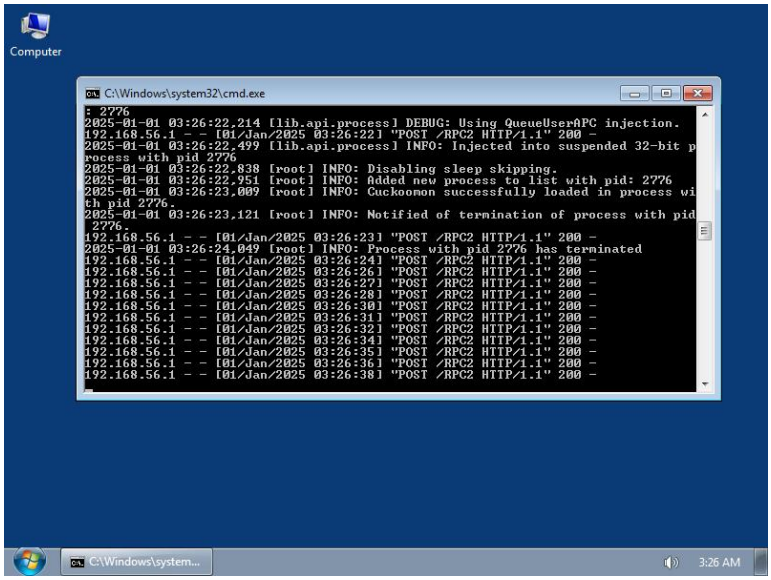

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:51] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

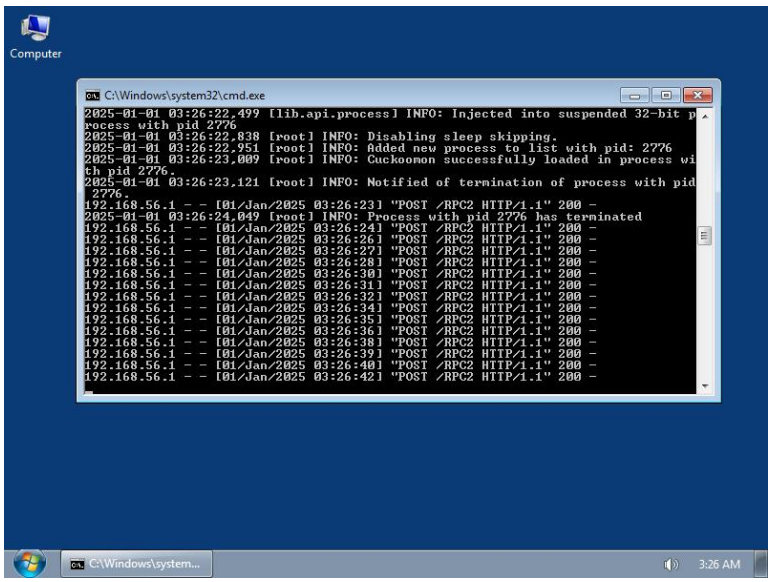

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:57] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

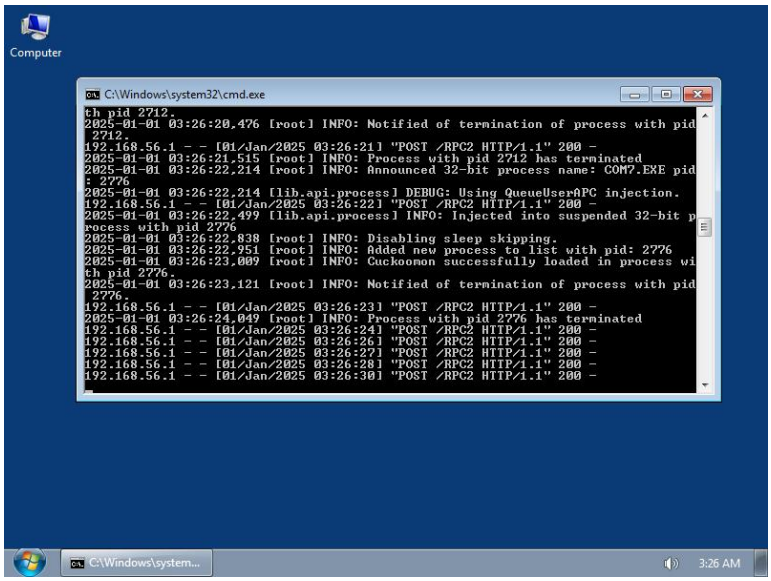

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:53] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

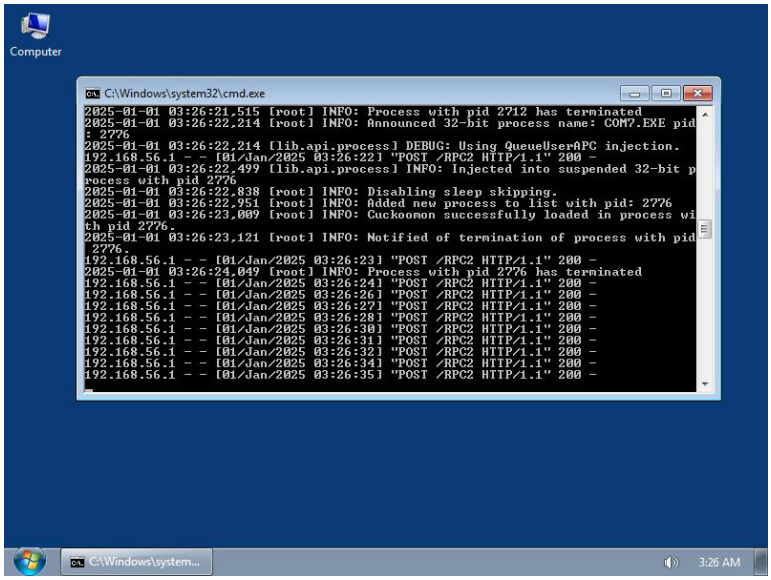

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:13] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:14,756 [root] INFO: Added new file to list with path: D:\Program Files\FoxitReader\bin\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:15,900 [root] INFO: Announced 32-bit process name: reg.exe pid: 2608
2025-01-01 03:26:15,900 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:15,918 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2608
2025-01-01 03:26:15,937 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:15,937 [root] INFO: Added new process to list with pid: 2608
2025-01-01 03:26:15,957 [root] INFO: Cuckoomon successfully loaded in process with pid 2608.
2025-01-01 03:26:15,957 [root] INFO: Notified of termination of process with pid 2608.
192.168.56.1 - - [01/Jan/2025 03:26:16] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:16,657 [root] INFO: Process with pid 2608 has terminated
2025-01-01 03:26:16,921 [root] INFO: Added new file to list with path: D:\Program Files\FoxitReader\FoxitReader.exe
192.168.56.1 - - [01/Jan/2025 03:26:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:18] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:18,868 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PDF FoxitReader.exe
C:\Windows\system...
3:26 AM

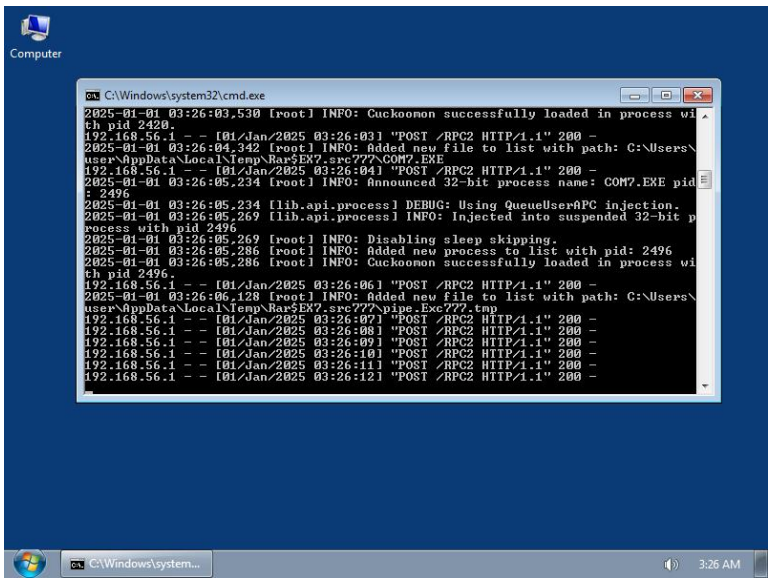

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:56] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:58] "POST /RPC2 HTTP/1.1" 200 -
Wednesday, January 01, 2025
C:\Windows\system...
3:26 AM

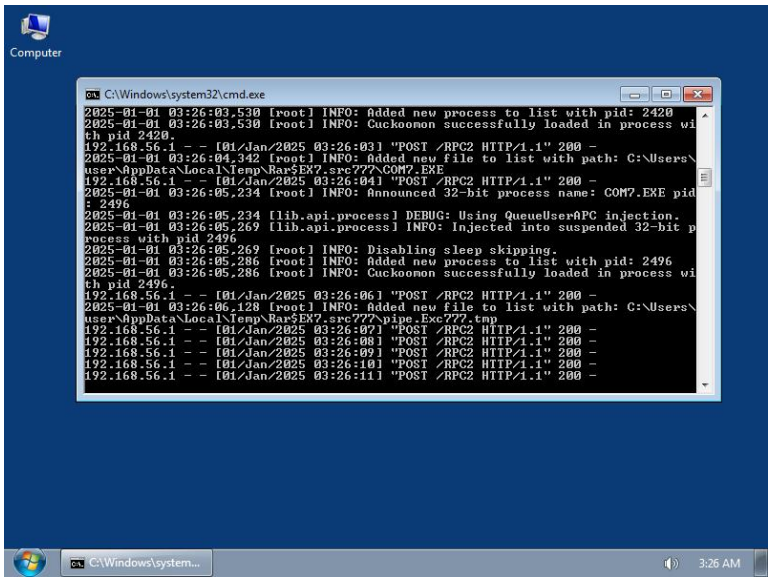

Computer
C:\Windows\system32\cmd.exe
: 2776
2025-01-01 03:26:22,214 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid
2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

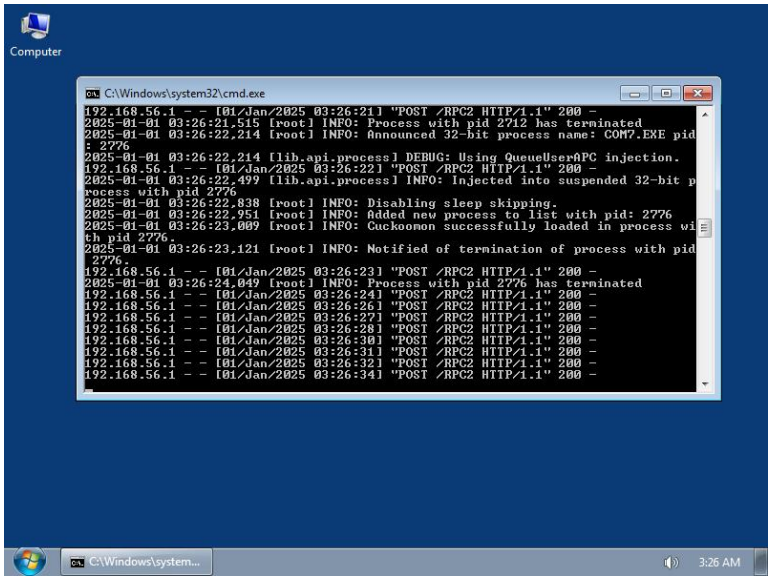

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid
2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

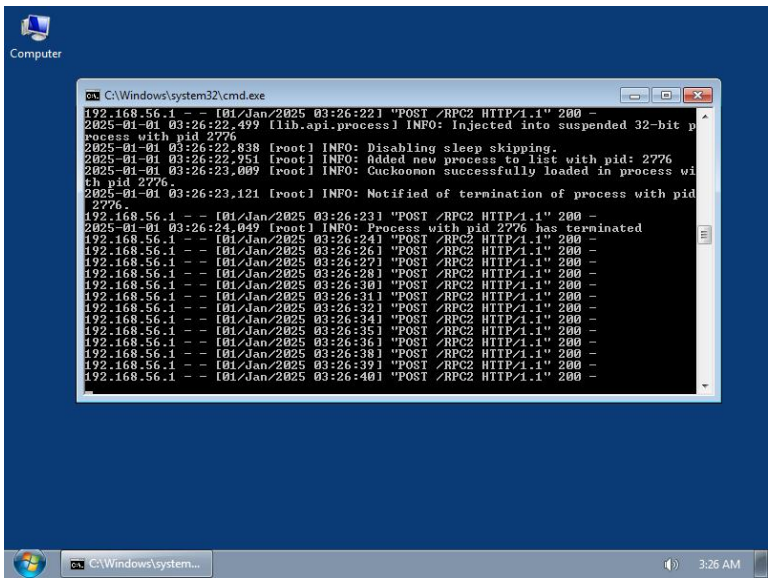

Computer
C:\Windows\system32\cmd.exe
th pid 2712.
2025-01-01 03:26:20,476 [root] INFO: Notified of termination of process with pid
2712.
192.168.56.1 - - [01/Jan/2025 03:26:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:21,515 [root] INFO: Process with pid 2712 has terminated
2025-01-01 03:26:22,214 [root] INFO: Announced 32-bit process name: COM7.EXE pid
: 2776
2025-01-01 03:26:22,214 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid
2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

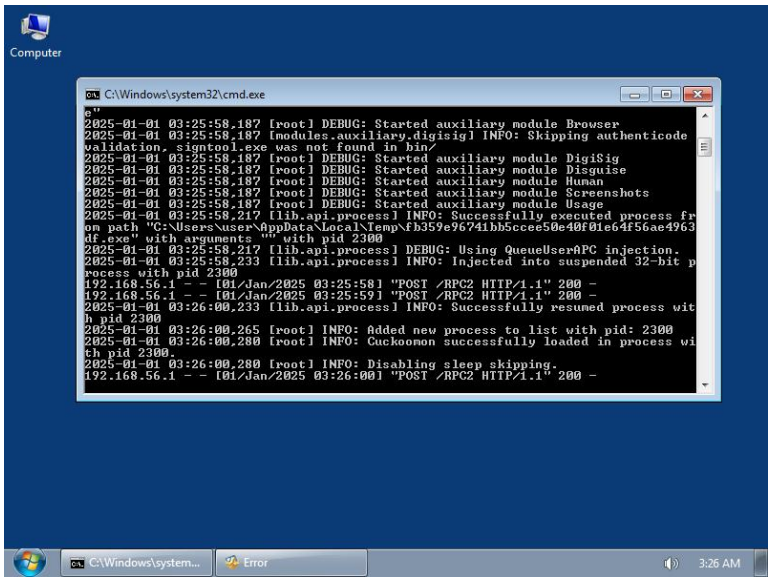

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:21,515 [root] INFO: Process with pid 2712 has terminated
2025-01-01 03:26:22,214 [root] INFO: Announced 32-bit process name: COM7.EXE pid
: 2776
2025-01-01 03:26:22,214 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid
2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

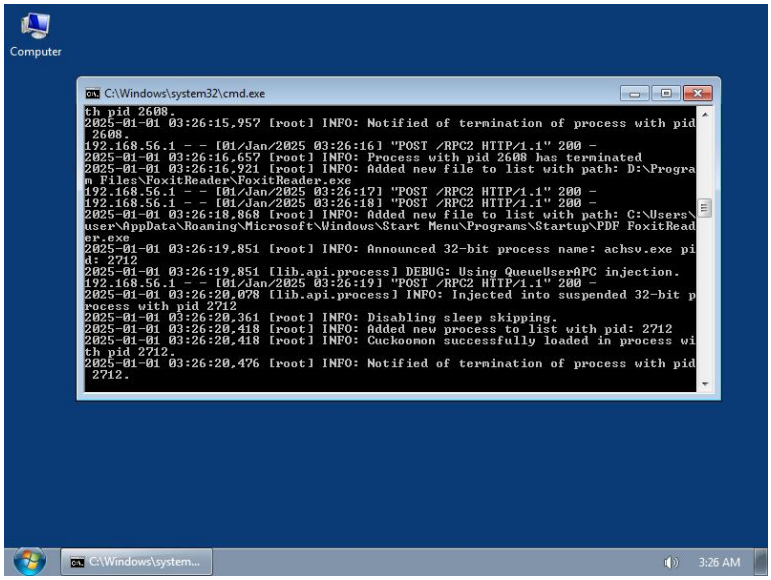

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:03,530 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2420.
192.168.56.1 - - [01/Jan/2025 03:26:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:04,342 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:04] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:05,234 [root] INFO: Announced 32-bit process name: COM7.EXE pid
: 2496
2025-01-01 03:26:05,234 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:05,269 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2496
2025-01-01 03:26:05,269 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:05,286 [root] INFO: Added new process to list with pid: 2496
2025-01-01 03:26:05,286 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2496.
192.168.56.1 - - [01/Jan/2025 03:26:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:06,128 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Rar$EX7.src777\pipe.Exc777.tmp
192.168.56.1 - - [01/Jan/2025 03:26:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:12] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

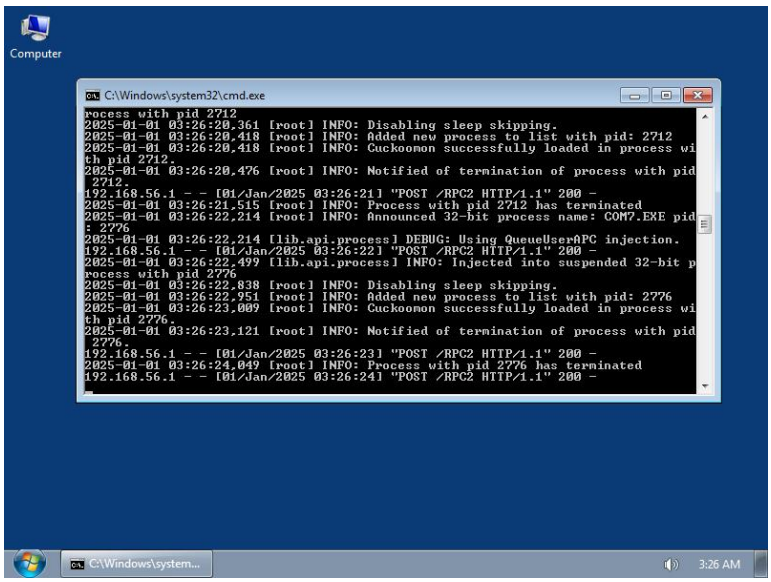

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:03,530 [root] INFO: Added new process to list with pid: 2420
2025-01-01 03:26:03,530 [root] INFO: Cuckoomon successfully loaded in process with pid 2420.
192.168.56.1 - - [01/Jan/2025 03:26:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:04,342 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:04] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:05,234 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2496
2025-01-01 03:26:05,234 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:05,269 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2496
2025-01-01 03:26:05,269 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:05,286 [root] INFO: Added new process to list with pid: 2496
2025-01-01 03:26:05,286 [root] INFO: Cuckoomon successfully loaded in process with pid 2496.
192.168.56.1 - - [01/Jan/2025 03:26:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:06,128 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\pipe.Exe777.tmp
192.168.56.1 - - [01/Jan/2025 03:26:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:11] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

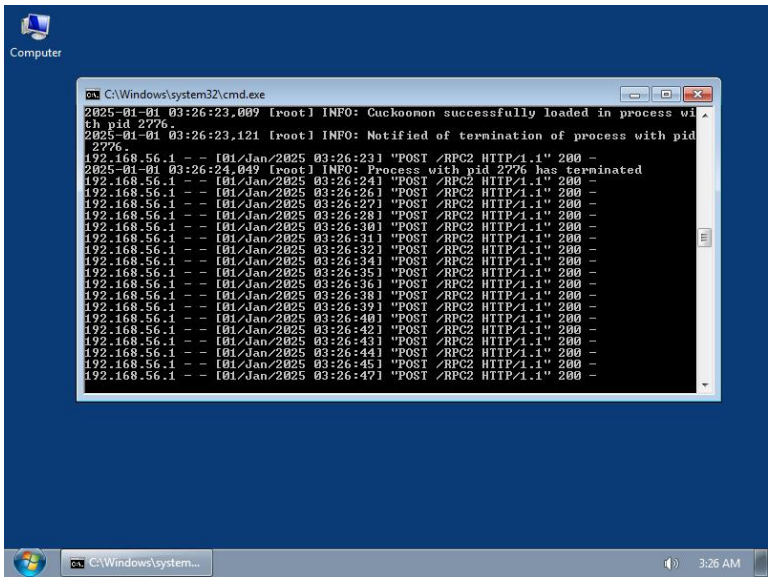

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:21,515 [root] INFO: Process with pid 2712 has terminated
2025-01-01 03:26:22,214 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2776
2025-01-01 03:26:22,214 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process with pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid 2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

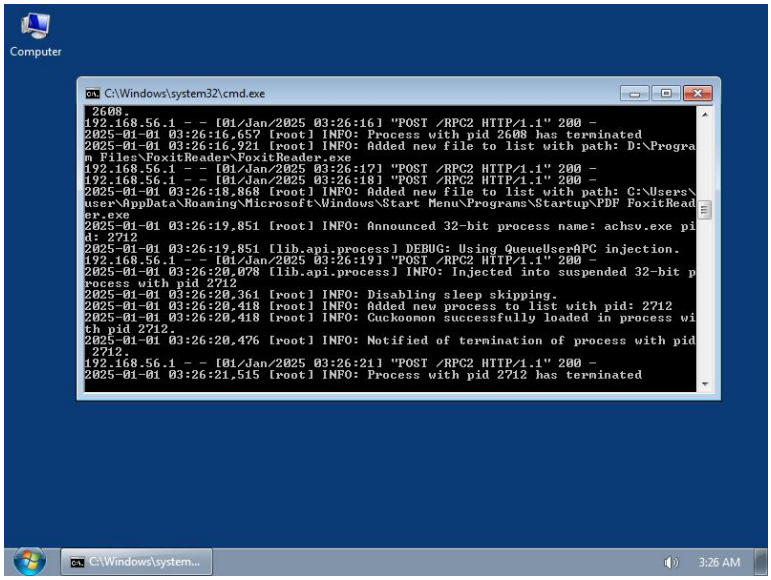

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process with pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid 2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

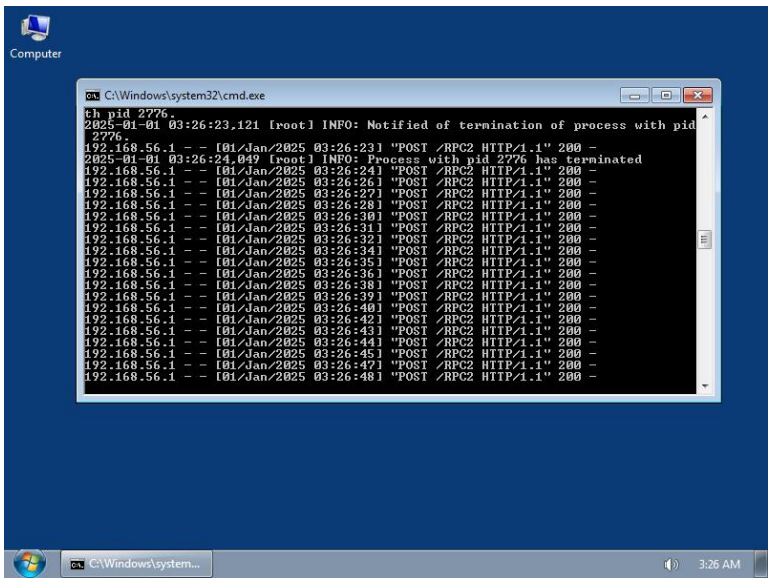

Computer
C:\Windows\system32\cmd.exe
e"
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Browser
2025-01-01 03:25:58,187 [modules.auxiliary.digisig] INFO: Skipping authenticode validation, signtool.exe was not found in bin/
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module DigiSig
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Disguise
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Human
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Screenshots
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Usage
2025-01-01 03:25:58,217 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\fb359e96741bb5ccee50e40f01e64f56ae4963df.exe" with arguments "" with pid 2300
2025-01-01 03:25:58,217 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:25:58,233 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2300
192.168.56.1 - - [01/Jan/2025 03:25:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:25:59] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:00,233 [lib.api.process] INFO: Successfully resumed process with pid 2300
2025-01-01 03:26:00,265 [root] INFO: Added new process to list with pid: 2300
2025-01-01 03:26:00,280 [root] INFO: Cuckoomon successfully loaded in process with pid 2300.
2025-01-01 03:26:00,280 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [01/Jan/2025 03:26:00] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Error
3:26 AM

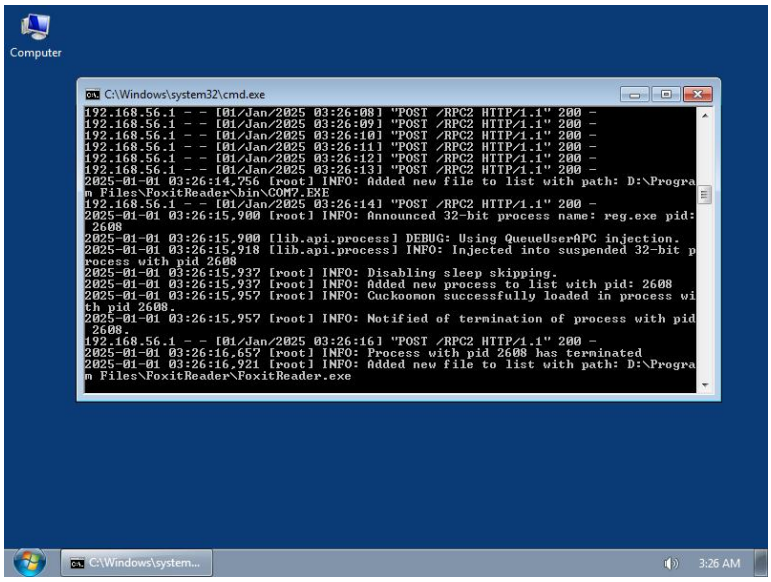

Computer
C:\Windows\system32\cmd.exe
th pid 2608.
2025-01-01 03:26:15,957 [root] INFO: Notified of termination of process with pid 2608.
192.168.56.1 - - [01/Jan/2025 03:26:16] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:16,657 [root] INFO: Process with pid 2608 has terminated
2025-01-01 03:26:16,921 [root] INFO: Added new file to list with path: D:\Program Files\FoxitReader\FoxitReader.exe
192.168.56.1 - - [01/Jan/2025 03:26:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:18] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:18,868 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PDF FoxitReader.exe
2025-01-01 03:26:19,851 [root] INFO: Announced 32-bit process name: achsv.exe pid: 2712
2025-01-01 03:26:19,851 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:19] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:20,078 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2712
2025-01-01 03:26:20,361 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:20,418 [root] INFO: Added new process to list with pid: 2712
2025-01-01 03:26:20,418 [root] INFO: Cuckoomon successfully loaded in process with pid 2712.
2025-01-01 03:26:20,476 [root] INFO: Notified of termination of process with pid 2712.
C:\Windows\system...
3:26 AM

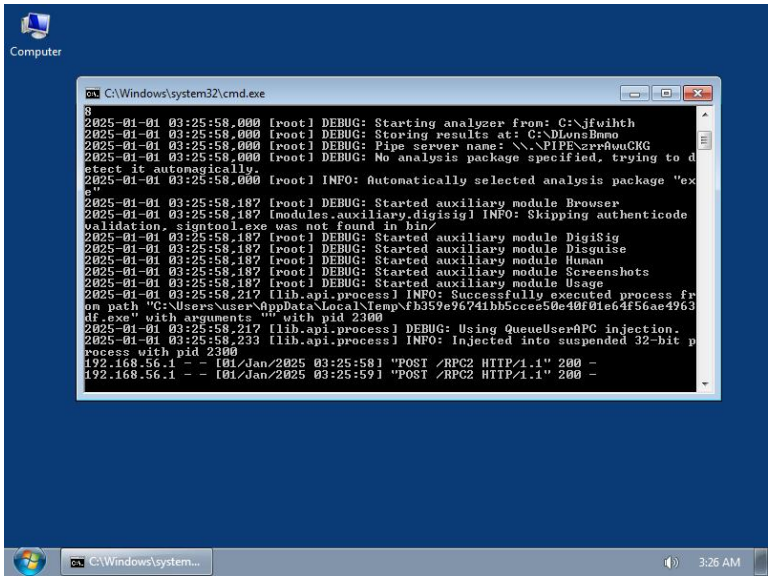

Computer
C:\Windows\system32\cmd.exe
rocess with pid 2712
2025-01-01 03:26:20,361 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:20,418 [root] INFO: Added new process to list with pid: 2712
2025-01-01 03:26:20,418 [root] INFO: Cuckoomon successfully loaded in process with pid 2712.
2025-01-01 03:26:20,476 [root] INFO: Notified of termination of process with pid 2712.
192.168.56.1 - - [01/Jan/2025 03:26:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:21,515 [root] INFO: Process with pid 2712 has terminated
2025-01-01 03:26:22,214 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2776
2025-01-01 03:26:22,214 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:22] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:22,499 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2776
2025-01-01 03:26:22,838 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:22,951 [root] INFO: Added new process to list with pid: 2776
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process with pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid 2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

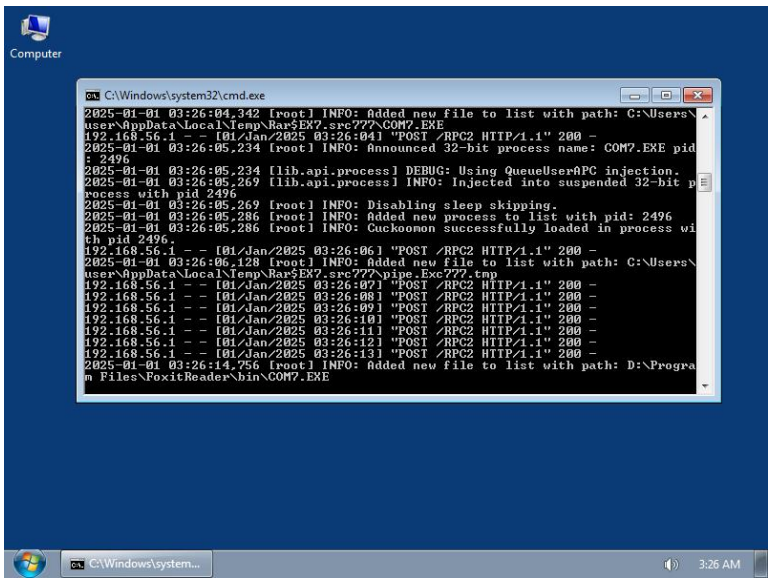

Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:23,009 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid
2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM

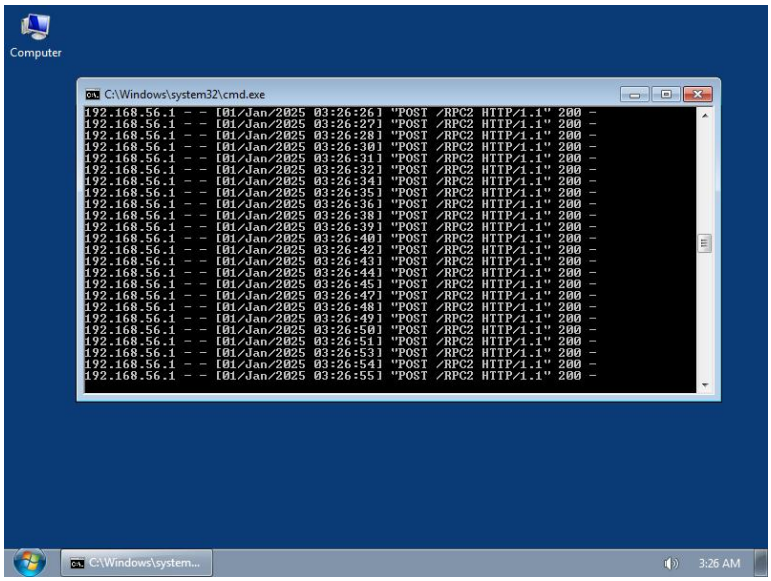

Computer
C:\Windows\system32\cmd.exe
2608.
192.168.56.1 - - [01/Jan/2025 03:26:16] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:16,657 [root] INFO: Process with pid 2608 has terminated
2025-01-01 03:26:16,921 [root] INFO: Added new file to list with path: D:\Progra
m Files\FoxitReader\FoxitReader.exe
192.168.56.1 - - [01/Jan/2025 03:26:17] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:18] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:18,868 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\PDF FoxitRead
er.exe
2025-01-01 03:26:19,851 [root] INFO: Announced 32-bit process name: achsv.exe pi
d: 2712
2025-01-01 03:26:19,851 [lib.api.process] DEBUG: Using QueueUserAPC injection.
192.168.56.1 - - [01/Jan/2025 03:26:19] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:20,078 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2712
2025-01-01 03:26:20,361 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:20,418 [root] INFO: Added new process to list with pid: 2712
2025-01-01 03:26:20,418 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2712.
2025-01-01 03:26:20,476 [root] INFO: Notified of termination of process with pid
2712.
192.168.56.1 - - [01/Jan/2025 03:26:21] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:21,515 [root] INFO: Process with pid 2712 has terminated
C:\Windows\system...
3:26 AM

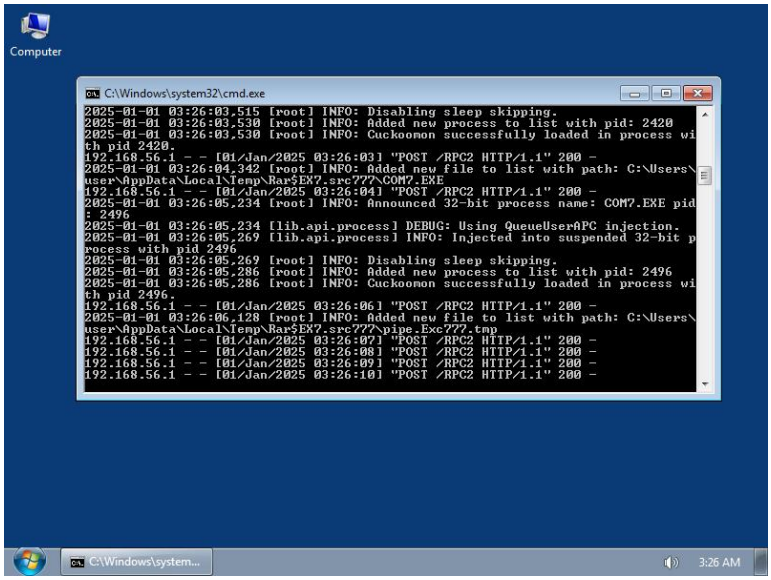

Computer
C:\Windows\system32\cmd.exe
th pid 2776.
2025-01-01 03:26:23,121 [root] INFO: Notified of termination of process with pid
2776.
192.168.56.1 - - [01/Jan/2025 03:26:23] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:24,049 [root] INFO: Process with pid 2776 has terminated
192.168.56.1 - - [01/Jan/2025 03:26:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:48] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM


Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:13] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:14,756 [root] INFO: Added new file to list with path: D:\Program Files\FoxitReader\bin\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:14] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:15,900 [root] INFO: Announced 32-bit process name: reg.exe pid: 2608
2025-01-01 03:26:15,900 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:15,918 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2608
2025-01-01 03:26:15,937 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:15,937 [root] INFO: Added new process to list with pid: 2608
2025-01-01 03:26:15,957 [root] INFO: Cuckoomon successfully loaded in process with pid 2608.
2025-01-01 03:26:15,957 [root] INFO: Notified of termination of process with pid 2608.
192.168.56.1 - - [01/Jan/2025 03:26:16] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:16,657 [root] INFO: Process with pid 2608 has terminated
2025-01-01 03:26:16,921 [root] INFO: Added new file to list with path: D:\Program Files\FoxitReader\FoxitReader.exe
C:\Windows\system...
3:26 AM


Computer
C:\Windows\system32\cmd.exe
8
2025-01-01 03:25:58,000 [root] DEBUG: Starting analyzer from: C:\jfwihth
2025-01-01 03:25:58,000 [root] DEBUG: Storing results at C:\DLwnsBmwo
2025-01-01 03:25:58,000 [root] DEBUG: Pipe server name: \\.\PIPE\zrrAwuCKG
2025-01-01 03:25:58,000 [root] DEBUG: No analysis package specified, trying to detect it automagically.
2025-01-01 03:25:58,000 [root] INFO: Automatically selected analysis package "exe"
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Browser
2025-01-01 03:25:58,187 [modules.auxiliary.digisig] INFO: Skipping authenticode validation, signtool.exe was not found in bin/
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module DigiSig
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Disguise
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Human
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Screenshots
2025-01-01 03:25:58,187 [root] DEBUG: Started auxiliary module Usage
2025-01-01 03:25:58,217 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\fb359e96741bb5ccee50e40f01e64f56ae4963df.exe" with arguments "" with pid 2300
2025-01-01 03:25:58,217 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:25:58,233 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2300
192.168.56.1 - - [01/Jan/2025 03:25:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:25:59] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM


Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:04,342 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:04] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:05,234 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2496
2025-01-01 03:26:05,234 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:05,269 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2496
2025-01-01 03:26:05,269 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:05,286 [root] INFO: Added new process to list with pid: 2496
2025-01-01 03:26:05,286 [root] INFO: Cuckoomon successfully loaded in process with pid 2496.
192.168.56.1 - - [01/Jan/2025 03:26:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:06,128 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\pipe.Exe777.tmp
192.168.56.1 - - [01/Jan/2025 03:26:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:11] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:13] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:14,756 [root] INFO: Added new file to list with path: D:\Program Files\FoxitReader\bin\COM7.EXE
C:\Windows\system...
3:26 AM


Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [01/Jan/2025 03:26:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:31] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:35] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:40] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:43] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:49] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:53] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:55] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM


Computer
C:\Windows\system32\cmd.exe
2025-01-01 03:26:03,515 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:03,530 [root] INFO: Added new process to list with pid: 2420
2025-01-01 03:26:03,530 [root] INFO: Cuckoomon successfully loaded in process with pid 2420.
192.168.56.1 - - [01/Jan/2025 03:26:03] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:04,342 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\COM7.EXE
192.168.56.1 - - [01/Jan/2025 03:26:04] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:05,234 [root] INFO: Announced 32-bit process name: COM7.EXE pid: 2496
2025-01-01 03:26:05,234 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2025-01-01 03:26:05,269 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2496
2025-01-01 03:26:05,269 [root] INFO: Disabling sleep skipping.
2025-01-01 03:26:05,286 [root] INFO: Added new process to list with pid: 2496
2025-01-01 03:26:05,286 [root] INFO: Cuckoomon successfully loaded in process with pid 2496.
192.168.56.1 - - [01/Jan/2025 03:26:06] "POST /RPC2 HTTP/1.1" 200 -
2025-01-01 03:26:06,128 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Rar$EX7.src777\pipe.Exc777.tmp
192.168.56.1 - - [01/Jan/2025 03:26:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:09] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [01/Jan/2025 03:26:10] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
3:26 AM