VALKYRIE COMODO

Summary

File Name: 4598044bb8a3a25bac91e2a069062dce89fb7dfd

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

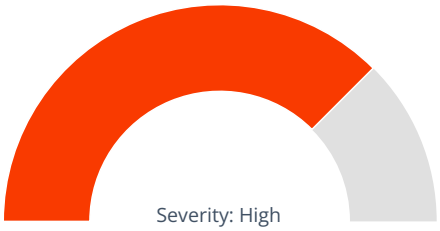
SHA1: 4598044bb8a3a25bac91e2a069062dce89fb7dfd

MD5: bc864bf3e7bf03bf665eb4e782989471

MALWARE

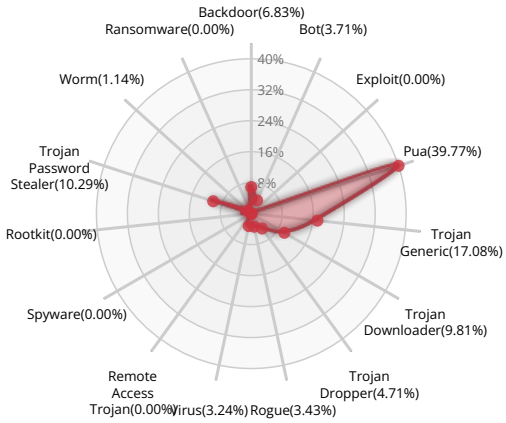
Valkyrie Final Verdict

DETECTION SECTION

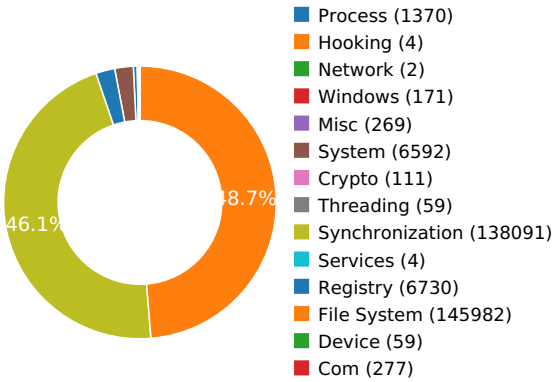


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image — Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Creates a copy of itself — Show sources

MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task. — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to block SafeBoot use by removing registry keys — Show sources

Behavior Graph

13:48:21 **13:48:57** **13:49:33**

PID 2240

13:48:21	**Create Process**	The malicious file created a child process as 4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe **(PPID 2180)**

13:48:21 13:48:22	NtReadFile **[12 times]**
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process

13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process

13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process

13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process

13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process

13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process

13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:21	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process

13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process
13:48:22	Create Process

13:48:22 Create Process

13:48:22 Create Process

PID 2428

13:48:22 **Create Process** The malicious file created a child process as powershell.exe **(PPID 2240)**

13:48:22 NtAllocateVirtualMem

13:48:24 NtDelayExecution

13:49:33 Create Process

PID 556

13:48:34 **Create Process** The malicious file created a child process as svchost.exe **(PPID 452)**

13:48:40 Create Process

PID 2076

13:48:41 **Create Process** The malicious file created a child process as WmiPrvSE.exe **(PPID 556)**

PID 2732

13:48:38 **Create Process** The malicious file created a child process as svchost.exe **(PPID 452)**

13:48:40 RegOpenKeyExW

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\nsu9598.tmp
C:\Users\user\AppData\Local\Temp\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
C:\Windows\Fonts\staticcache.dat
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp\Stilstandsperioden
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\henrykket.dll
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Penanced.Spg
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Popelike
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Popelike\asexuality.Laa
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Popelike\afvrgningen.sky
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Popelike\Conscionable
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Popelike\Conscionable\blameres.voc
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Popelike\Conscionable\constituter.tab
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Popelike\Conscionable\stdfanger.att
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\tyvestykspakken.usm
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\viceamtsborgmestrene.txt
C:\Users\user\Documents\ficelle.Sld
C:\Users\user\Pictures\Bedkkende223.far
C:\Windows\Fonts\erhversindkomsten.Uor
C:\Users\user\AppData\Roaming\Microsoft\Windows\Templates\Knibtangsbevgelser137\overage.per
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\uddannelsesfiler
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files

C:\Users\user\AppData\Local\Microsoft\Windows
C:\Users\user\AppData\Local\Microsoft
C:\
C:\Users\user\AppData\Local\Temp\peroxiding.ini
C:\Users\Public
C:\Users\Public\Videos
C:\Users\Public\Videos\personificerer
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\sksporen.sun
C:\ProgramData\Microsoft\Windows\Templates\Knibtangsbevgelser137\overage.per
C:\Users\user*.imi
C:\Users\Public\Videos\alfred.ini
C:\Windows\System32\bortfragterne.con
C:\Users\Public\Pictures\Bedkkende223.far
C:\konstantvrdiers.Tra
C:\Users\Public\Pictures\symbiotes\Isled.Upu
C:\Users\Public\Music\ressourcegrnsen.Sta210
C:\Program Files (x86)\overreactions\Sammenknytningernes.cha
C:\Windows\synftigstes\ambivalensens.bas
C:\Users\Public\Documents\Arbejdsstationers224.raa
C:\Users\user\plagsommere\henvisningsstregernes.ini
C:\Windows\Fonts\catamnestic\Velgrenheden.non
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\portraitlike.Cur
C:\Windows\Fonts\Tampningens40\fatamorganaernes.ini
C:\Users\user\wore
C:\Users\user\wore\Styresystems163.sco
\??\Volume{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
C:\Users\user\stimulis.lnk
C:\Users\Public\Documents\ficelle.Sld
C:\Users\user\elementre\Stigerne.fol
C:\Windows\System32\UXTHEME.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Program Files (x86)\Spildevandsplanen204\Herman155.ini
C:\Users\user\parre.ini

C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
C:\Windows
C:\Windows\SysWOW64
C:\Windows\SysWOW64\WindowsPowerShell\v1.0
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
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.ver0x000000000000004c.db
C:\Users\desktop.ini

READ REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewShadow
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AccListViewV6
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ProgramFilesDir
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\AllowFileCLSIDJunctions
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\User Shell Folders\Common Desktop
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\{DE92C1C7-837F-4F69-A3BB-86E631204A23}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\My Music
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\User Shell Folders\{3D644C9B-1FB8-4F30-9B45-F670235F79C0}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\ProfilesDirectory
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Startup
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\User Shell Folders\Common Startup
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\Public
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\Programs
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\User Shell Folders\Common Programs
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\CommonFilesDir
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\{52A4F021-7B75-48A9-9F6B-4B87A210BC8F}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesMyComputer

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoPropertiesRecycleBin
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoControlPanel
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoSetFolders
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoInternetIcon
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoCommonGroups
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Category
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Name
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParentFolder
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Description
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\RelativePath
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\ParsingName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\InfoTip
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalizedName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Icon
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Security
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResource
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\StreamResourceType
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\LocalRedirectOnly
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\FolderDescriptions\{625B53C3-AB48-4EC1-BA1F-A1EF4146FC19}\Roamable

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Penanced.Spg
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Popelike\asexuality.Laa
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Popelike\afvrgningen.sky
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Popelike\Conscionable\blameres.voc
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Popelike\Conscionable\constituter.tab
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Popelike\Conscionable\stdfanger.att
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\tyvestykspakken.usm

C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\viceamtsborgmestrene.txt
C:\Users\user\AppData\Local\Temp\peroxiding.ini
C:\Users\Public\Videos\alfred.ini
C:\Program Files (x86)\overreactions\Sammenknytningernes.cha
C:\Users\user\plagsommere\henvisningsstregernes.ini
C:\Windows\Fonts\Tampningens40\fatamorganaernes.ini
C:\Users\user\stimulis.lnk
C:\Program Files (x86)\Spildevandsplanen204\Herman155.ini
C:\Users\user\parre.ini
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
\??\PIPE\srvsvc
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3IMKYONZM3Y5AET7ROQO.temp
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
C:\Users\user\AppData\Local\Temp\OutofProcReport17888571.txt
\??\PIPE\samr
C:\Windows\sysnative\wbem\repository\WRITABLE.TST
C:\Windows\sysnative\wbem\repository\MAPPING1.MAP
C:\Windows\sysnative\wbem\repository\MAPPING2.MAP
C:\Windows\sysnative\wbem\repository\MAPPING3.MAP
C:\Windows\sysnative\wbem\repository\OBJECTS.DATA
C:\Windows\sysnative\wbem\repository\INDEX.BTR
\??\pipe\PIPE_EVENTROOT\CIMV2WMI SELF-INSTRUMENTATION EVENT PROVIDER
\??\pipe\PIPE_EVENTROOT\CIMV2PROVIDERSUBSYSTEM

RESOLVED APIS

version.dll.GetFileVersionInfoA
shfolder.dll.SHGetFolderPathA
shlwapi.dll.#437
cryptbase.dll.SystemFunction036
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
comctl32.dll.#386

kernel32.dll.GetUserDefaultUILanguage
dwmapi.dll.DwmIsCompositionEnabled
comctl32.dll.RegisterClassNameW
uxtheme.dll.EnableThemeDialogTexture
uxtheme.dll.OpenThemeData
uxtheme.dll.GetThemeBool
uxtheme.dll.GetThemeInt
uxtheme.dll.IsThemePartDefined
uxtheme.dll.GetThemePartSize
uxtheme.dll.GetThemeFont
uxtheme.dll.GetThemeColor
imm32.dll.ImmIsIME
uxtheme.dll.CloseThemeData
uxtheme.dll.GetThemeTextExtent
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
uxtheme.dll.GetThemeMargins
gdi32.dll.GdiIsMetaPrintDC
ole32.dll.CoInitializeEx
ole32.dll.CoUninitialize
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoRevokeInitializeSpy
uxtheme.dll.BufferedPaintInit
uxtheme.dll.BufferedPaintRenderAnimation

uxtheme.dll.BeginBufferedAnimation
uxtheme.dll.IsThemeBackgroundPartiallyTransparent
uxtheme.dll.DrawThemeParentBackground
uxtheme.dll.DrawThemeBackground
uxtheme.dll.GetThemeBackgroundContentRect
uxtheme.dll.DrawThemeText
uxtheme.dll.EndBufferedAnimation
uxtheme.dll.DrawThemeParentBackgroundEx
propsys.dll.PSCreateMemoryPropertyStore
comctl32.dll.HIMAGELIST_QueryInterface
comctl32.dll.DrawShadowText
comctl32.dll.DrawSizeBox
comctl32.dll.DrawScrollBar
comctl32.dll.SizeBoxHwnd
comctl32.dll.ScrollBar_MouseMove
comctl32.dll.ScrollBar_Menu
comctl32.dll.HandleScrollCmd
comctl32.dll.DetachScrollBars
comctl32.dll.AttachScrollBars
comctl32.dll.CCSetScrollInfo
comctl32.dll.CCGetScrollInfo
comctl32.dll.CCEnableScrollBar
comctl32.dll.QuerySystemGestureStatus
uxtheme.dll.#49
ole32.dll.CoCreateInstance
shell32.dll.#66
ole32.dll.CoGetApartmentType
ole32.dll.CoTaskMemFree
comctl32.dll.#236
oleaut32.dll.#6
ole32.dll.CoTaskMemAlloc
ole32.dll.CoGetMalloc
ole32.dll.CreateBindCtx

DELETED FILES

C:\Users\user\AppData\Local\Temp\nsu9598.tmp
C:\Users\Public\Music\ressourcegrnsen.Sta210
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3IMKYONZM3Y5AET7ROQO.temp
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch.2428.16859484
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch.2428.16859484
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch.2428.16859484

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_CURRENT_USER
HKEY_CURRENT_USER\Control Panel\Desktop
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewShadow

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AccListViewV6
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\MS Shell Dlg 2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\thimblesful\Uninstall\rambler\oprrsstyrkens

HKEY_LOCAL_MACHINE\tjenesterejser\proteser\ekstraversioners
HKEY_CURRENT_USER\Tusindfoldige\
HKEY_LOCAL_MACHINE\ghastlily\samuelsen
HKEY_CURRENT_USER\majos\chalana\licking
HKEY_LOCAL_MACHINE\checker\unrumoreds
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\SESSION MANAGER\SafeProcessSearchMode
HKEY_LOCAL_MACHINE\hidtil\lecithalbumin\arvebeholdning
HKEY_LOCAL_MACHINE\omstdelsesregels\dokumentnavn\idols
HKEY_CURRENT_USER\Skovranken\trafikstjens
HKEY_LOCAL_MACHINE\klag\balfaldera\Bulkskib
HKEY_LOCAL_MACHINE\Unrequitable\Gstetoilet\Kolonneblokkes
HKEY_CURRENT_USER\lanceman\Sniffe\
HKEY_CURRENT_USER\sleekest\Mesole
HKEY_CURRENT_USER\sleekest\Mesole\ethmonasal
HKEY_LOCAL_MACHINE\udsttelsesbegringen\Uninstall\passagerskib
HKEY_CURRENT_USER\saviors\Uninstall\chansonernes
HKEY_CURRENT_USER\saviors\Uninstall\chansonernes\purporters

EXECUTED COMMANDS

"C:\Users\user\Videos\lungworms.Sys"
"C:\Users\user\Videos\dentalizing.afs"
"C:\Windows\Fonts\uncontributory\millile.aab"
"C:\Users\Public\Videos\dentalizing.afs"
"C:\Users\Public\Videos\lungworms.Sys"
"C:\Windows\system32\wermgr.exe" "-outproc" "2428" "1124"
C:\Windows\system32\wbem\wmiprvse.exe -secured -Embedding

READ FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\nsu9598.tmp
C:\Users\user\AppData\Local\Temp\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\peroxiding.ini
C:\Users\Public\Videos\alfred.ini
C:\Users\user\plagsommere\henvisningsstregernes.ini

C:\Windows\Fonts\Tampningens40\fatamorganaernes.ini
C:\
C:\Users
C:\Users\user
C:\Users\user\stimulis.lnk
C:\Windows\System32\UXTHEME.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Program Files (x86)\Spildevandsplanen204\Herman155.ini
C:\Users\user\parre.ini
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\cversions.1.db
C:\Users\user\AppData\Local\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.ver0x000000000000004c.db
C:\Users\desktop.ini
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\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\ProgramData
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\Public\desktop.ini
C:\Users\Public
C:\Users\Public\Desktop\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Windows\System32\shdocvw.dll

C:\Windows\AppPatch\sysmain.sdb
C:\Windows\System32\
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms
C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk
C:\Windows\%ProgramData%\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\Windows PowerShell.lnk\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell\desktop.ini
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Windows PowerShell
\??\PIPE\srvsvc
C:\Windows
C:\Windows\System32
C:\Windows\System32\WindowsPowerShell
C:\Windows\System32\WindowsPowerShell\v1.0
C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3IMKYONZM3Y5AET7ROQO.temp
C:\Windows\Microsoft.NET\Framework\v4.0.30319\mscoreei.dll
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\mscorwks.dll
C:\Windows\winsxs\x86_microsoft.vc80.crt_1fc8b3b9a1e18e3b_8.0.50727.4940_none_d08cc06a442b34fc\msvcr80.dll
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\security.config.cch
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\enterprisesec.config.cch
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config
C:\Users\user\AppData\Roaming\Microsoft\CLR Security Config\v2.0.50727.312\security.config.cch
C:\Windows\assembly\NativeImages_v2.0.50727_32\index12a.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\mscorlib\62a0b3e4b40ec0e8c5cfaa0c8848e64a\mscorlib.ni.dll
C:\Windows\assembly\pubpol20.dat
C:\Windows\assembly\NativeImages_v2.0.50727_32\System\9e0a3b9b9f457233a335d7fba8f95419\System.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.PowerShel#\b1c511d8fad78ad3c5213b2b4fb02b8b\Microsoft.PowerShell.ConsoleHost.ni.dll
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll
C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Management.A#\4436815b432c313255af322f4ec3560d\System.Management.Automation.ni.dll

MUTEXES

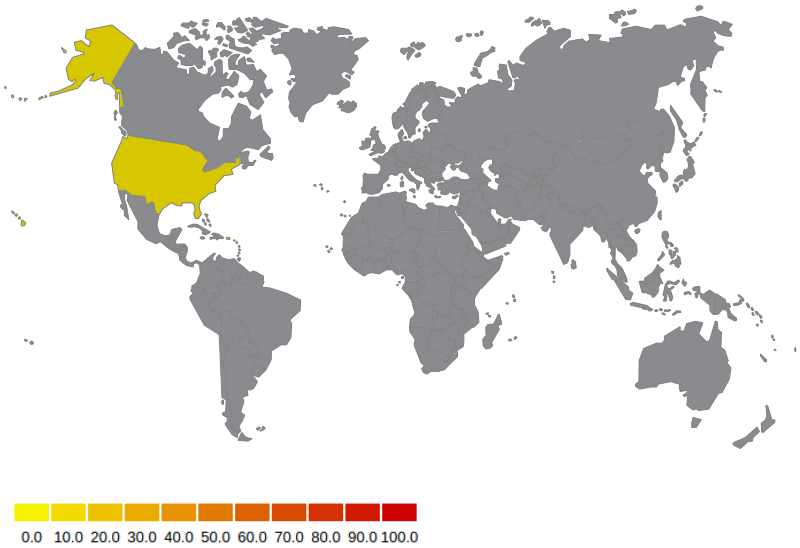
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Global\CLR_CASOFF_MUTEX
Global\f61ec9db-3879-11ef-9f13-0800275ed07b

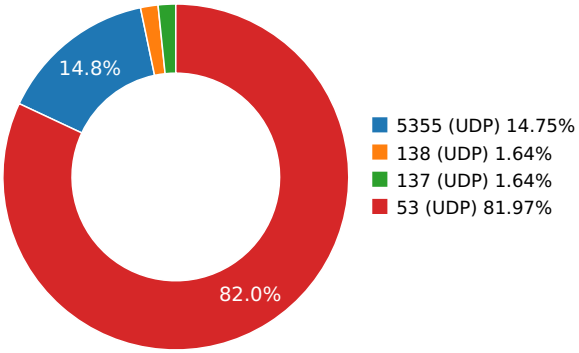
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\sleekest\Mesole
HKEY_CURRENT_USER\sleekest\Mesole\ethmonasal
HKEY_CURRENT_USER\saviors\Uninstall\chansonernes
HKEY_CURRENT_USER\saviors\Uninstall\chansonernes\purporters
HKEY_CURRENT_USER\seminarielrernes\slapperen\festspils
HKEY_CURRENT_USER\seminarielrernes\slapperen\festspils\kobbersulfat
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\LastServiceStart
HKEY_LOCAL_MACHINE\Software\Microsoft\Wbem\Transports\Decoupled\Server
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\CreationTime
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\MarshaledProxy
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\Transports\Decoupled\Server\ProcessIdentifier
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\ConfigValueEssNeedsLoading
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\List of event-active namespaces

Network Behavior

CONTACTED IPS	NETWORK PORT DISTRIBUTION





Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Google LLC	Malware Process
	8.8.8.8	United States	15169	Google LLC	Malware Process
					Malware Process
www.aieov.com	45.79.19.196	United States	63949	Akamai Technologies, Inc.	Malware Process
www.msftncsi.com	23.221.239.217	United States	20940	Akamai Technologies, Inc.	Malware Process

DNS QUERIES

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

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.01039886475	Sandbox	224.0.0.252	5355
3.01068902016	Sandbox	224.0.0.252	5355
3.07817602158	Sandbox	192.168.56.255	137
4.54853796959	Sandbox	224.0.0.252	5355
5.5630428791	Sandbox	224.0.0.252	5355
7.11097979546	Sandbox	8.8.4.4	53
8.10982894897	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
8.1257109642	Sandbox	224.0.0.252	5355
9.07820296288	Sandbox	192.168.56.255	138
10.7430949211	Sandbox	224.0.0.252	5355
12.6302349567	Sandbox	8.8.4.4	53
13.3014419079	Sandbox	224.0.0.252	5355
13.6248548031	Sandbox	8.8.8.8	53
15.9067659378	Sandbox	224.0.0.252	5355
18.4694960117	Sandbox	224.0.0.252	5355
26.9847838879	Sandbox	8.8.8.8	53
27.9844369888	Sandbox	8.8.4.4	53
41.4227747917	Sandbox	8.8.8.8	53
42.4217238426	Sandbox	8.8.4.4	53
56.6581687927	Sandbox	8.8.8.8	53
57.6584849358	Sandbox	8.8.4.4	53
71.1099879742	Sandbox	8.8.8.8	53
72.1091668606	Sandbox	8.8.4.4	53
85.5485038757	Sandbox	8.8.8.8	53
86.546697855	Sandbox	8.8.4.4	53
103.837054968	Sandbox	8.8.8.8	53
104.828593969	Sandbox	8.8.4.4	53
118.228917837	Sandbox	8.8.8.8	53
119.219254971	Sandbox	8.8.4.4	53
132.593154907	Sandbox	8.8.8.8	53
133.578176022	Sandbox	8.8.4.4	53
150.908597946	Sandbox	8.8.8.8	53
151.906400919	Sandbox	8.8.4.4	53
165.314585924	Sandbox	8.8.8.8	53
166.31251502	Sandbox	8.8.4.4	53
179.727676868	Sandbox	8.8.8.8	53
180.71901679	Sandbox	8.8.4.4	53
198.028410912	Sandbox	8.8.8.8	53
199.015913963	Sandbox	8.8.4.4	53
212.424548864	Sandbox	8.8.8.8	53
213.422109842	Sandbox	8.8.4.4	53
226.785949945	Sandbox	8.8.8.8	53
227.78132081	Sandbox	8.8.4.4	53
245.065778971	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
246.06229496	Sandbox	8.8.4.4	53
259.460878849	Sandbox	8.8.8.8	53
260.453522921	Sandbox	8.8.4.4	53
273.830968857	Sandbox	8.8.8.8	53
274.828638792	Sandbox	8.8.4.4	53
292.173844814	Sandbox	8.8.8.8	53
293.172428846	Sandbox	8.8.4.4	53
306.537953854	Sandbox	8.8.8.8	53
307.531422853	Sandbox	8.8.4.4	53
320.920581818	Sandbox	8.8.8.8	53
321.906577826	Sandbox	8.8.4.4	53
335.183723927	Sandbox	8.8.8.8	53
336.171908855	Sandbox	8.8.4.4	53
349.562871933	Sandbox	8.8.8.8	53
350.54731679	Sandbox	8.8.4.4	53
363.91629982	Sandbox	8.8.8.8	53
364.906466007	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Stilstandsperioden\Shonkinite\Nigranilin\Enlarge\Tyvestykspakken.Usm	**Type :** data **MD5 :** 0ca43fbee7d2abb39b43c94ee8e8ec4d **SHA-1 :** f6db85130d436798e702ac03d916bef0c741af10 **SHA-256 :** f8fc13ac66b928106b826a62a99e7e2bf1b56ba9 **SHA-512 :** 15a0a6585d15f43706f765b28d70ac32c1a83803 **Size :** 1358.458 Kilobytes.
C:\Users\User\AppData\Local\Temp\Stilstandsperioden\Shonkinite\Nigranilin\Penanced.Spg	**Type :** data **MD5 :** 202e85bb7eed102f5872c9131514a1e0 **SHA-1 :** 83d5573b40affa6025ccbb30ee7483968d1ea9c5 **SHA-256 :** 7df9cafc683133f3a0170e0756c628c018ea9ac10 **SHA-512 :** 261f7b206dfbb554d575f22c1585db6e76196a37 **Size :** 339.747 Kilobytes.
C:\Users\User\AppData\Local\Temp\Stilstandsperioden\Shonkinite\Nigranilin\Popelike\Asexuality.Laa	**Type :** ASCII text, with very long lines, with no line terminators **MD5 :** 20d9cb6e9d2ce0561d7505080357ce46 **SHA-1 :** 4319e0c74dd8fcabc20e197d3e1da9d8e6e1777d **SHA-256 :** 26e9c7382888e8cd677a50fb29c49511d2a0f089 **SHA-512 :** 156d898a0830c2d76f40f1d370b7647563fe99c9 **Size :** 70.742 Kilobytes.
C:\Users\User\AppData\Local\Temp\Stilstandsperioden\Shonkinite\Nigranilin\Popelike\Conscionable\Constituter.Tab	**Type :** data **MD5 :** eaa237d37ab023920806d41b53966a12 **SHA-1 :** 94c40958ccfaf687300b9567773397bdaba34df4 **SHA-256 :** bcea8b90cb62764f7854485b99b2cf6e0e4296c7 **SHA-512 :** 77ea54707e9b1a22d18d2a283da5c5cc4eefc9d9 **Size :** 786.803 Kilobytes.
C:\Users\Public\Videos\Alfred.Ini	**Type :** ASCII text, with CRLF line terminators **MD5 :** 86a672b0d851a955ab58008405e43e36 **SHA-1 :** 4b838b4995cc79459676bbcb408e2f4a22ca8f68 **SHA-256 :** 3d97f1a3681b1cae3bb160880998fd26266fe20c **SHA-512 :** 29f05a772036bcefe7c697973f0b12a19a78b8cc8 **Size :** 0.057 Kilobytes.
C:\Users\User\AppData\Local\Temp\Stilstandsperioden\Shonkinite\Nigranilin\Popelike\Conscionable\Stdfanger.Att	**Type :** data **MD5 :** ba642b9b4faae9eb6e4da87cef2fab06 **SHA-1 :** 2870144d71f340338dac3dba02e79e2795a1f3db **SHA-256 :** 5909bc3251342bb256816768f706e9b1c0a6bb0 **SHA-512 :** 02863fac1c61e8ce1c645a6018354ce311cbad4b **Size :** 1062.122 Kilobytes.
C:\Users\User\AppData\Local\Temp\Stilstandsperioden\Shonkinite\Nigranilin\Popelike\Conscionable\Blameres.Voc	**Type :** data **MD5 :** 3022025d7d7820aa8c04bee9f14a998c **SHA-1 :** c2cf8b847045c0e834132eb97e00135edad164de **SHA-256 :** f0c4afa98590028b9d733a7f58555a840f66357c4 **SHA-512 :** 760841a841048bc6056ea624adbe217e7245735 **Size :** 1180.58 Kilobytes.

FILE PATH	TYPE AND HASHES
C:\Users\User\Stimulis.Lnk	**Type :** MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Mon Jan 1 00:00:00 1601, mtime=Mon Jan 1 00:00:00 1601, atime=Mon Jan 1 00:00:00 1601, length=0, window=hide **MD5 :** 139da318b1b5eafbdb7a521ff29ea298 **SHA-1 :** 7e99e9824f3327f811e09ffde3f359ea5088e910 **SHA-256 :** 9e85b46ee77e9463821f2ed32277c497de6a9b0 **SHA-512 :** b77a7de8f676db3eaf279bddbdea06b3f7d79352 **Size :** 0.882 Kilobytes.
C:\Users\User\AppData\Local\Temp\Stilstandsperioden\Shonkinite\Nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive **MD5 :** bc864bf3e7bf03bf665eb4e782989471 **SHA-1 :** 4598044bb8a3a25bac91e2a069062dce89fb7dfd **SHA-256 :** 4b23416ddb5edceb2bcfd5c8b16fc0b739e2d47C **SHA-512 :** 2a9b9f5cca739f4d646668f556985f3873a37d049 **Size :** 944.24 Kilobytes.
C:\Users\User\AppData\Local\Temp\Stilstandsperioden\Shonkinite\Nigranilin\Enlarge\Viceamtsborgmestrene.Txt	**Type :** ASCII text, with CRLF line terminators **MD5 :** b485cf3f7554dcd671cdcba643ddbe62 **SHA-1 :** 49ad28e36f41192e61355686ad18e702af3f70f4 **SHA-256 :** 2f790220ed451fd4396f810746114e83a8a343d8 **SHA-512 :** a37b675fcad8153e528be4894a1195a5f774d306 **Size :** 0.452 Kilobytes.
C:\Users\User\AppData\Local\Temp\Stilstandsperioden\Shonkinite\Nigranilin\Popelike\Afvrgningen.Sky	**Type :** data **MD5 :** 08d01ed9939364dfbb50511c1ee29fd1 **SHA-1 :** e2b3f1dd281e24caa6767db4827215d838d87e7a **SHA-256 :** 51f2428993917da5647765e0f98406e2f706588a **SHA-512 :** 707358660ba7194b45d5ea93e895cf399b4993e **Size :** 600.587 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\D93f411851d7c929.CustomDestinations-Ms	**Type :** data **MD5 :** 37c5a48c4c2cd54efd968c398345cb44 **SHA-1 :** e33d66fd1b24b69e6de9953c51c7cd1bcdef13d3 **SHA-256 :** ae0f088fc172cf644a1d0e02d052a46ea4f63ea54 **SHA-512 :** 98f168ff40db9acbc34a3beb49599cd106e77930 **Size :** 8.016 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	4598044bb8a3a25bac91e2a069062dce89fb7dfd
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	4598044bb8a3a25bac91e2a069062dce89fb7dfd
MD5:	bc864bf3e7bf03bf665eb4e782989471
First Seen Date:	2024-07-01 16:56:17.147995 (about 22 hours ago)
Number Of Clients Seen:	4
Last Analysis Date:	2024-07-02 11:46:25.752459 (about 3 hours ago)
Human Expert Analysis Date:	2024-07-02 13:28:22.152832 (about 2 hours ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[[64.5, u'Win32 Executable MS Visual C++ (generic)'], [13.6, u'Win32 Dynamic Link Library (generic)'], [9.3, u'Win32 Executable (generic)'], [4.1, u'OS/2 Executable (generic)'], [4.1, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x5C157F01 [Sat Dec 15 22:24:01 2018 UTC]
ProductName	feerne
CompanyName	melders badian paleolithic
Translation	0x0409 0x04e4
Entry Point	0x4031e9 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	944240
Ssdeep	24576:rOGBWnfTjl004cgJkwrivQhUfSWSv+gCF9DR2sV:rxUTja09gaqqQhUxSM9V2s
Sha256	4b23416ddb5edceb2bcfd5c8b16fc0b739e2d470e69a7c85a033fbbedcac520f
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs-aws/fvs/valkyrie_shared/core/valkyrie_files/4/5/9/8/4598044bb8a3a25bac91e2a069062dce89fb7dfd', u'EXE:ProductName': u'feerne', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2024:07:01 12:55:36-04:00', u'EXE:InitializedDataSize': 3782656, u'File:FileModifyDate': u'2024:07:01 12:54:59-04:00', u'EXE:FileVersionNumber': u'1.4.0.0', u'File:FileSize': u'922 kB', u'EXE:CharacterSet': u'Windows, Latin1', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'melders badian paleolithic', u'File:FileName': u'4598044bb8a3a25bac91e2a069062dce89fb7dfd', u'EXE:ImageVersion': 6.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2018:12:15 17:24:01-05:00', u'EXE:FileFlagsMask': u'0x0000', u'EXE:LinkerVersion': 6.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs-aws/fvs/valkyrie_shared/core/valkyrie_files/4/5/9/8', u'EXE:EntryPoint': u'0x31e9', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 25088, u'File:FileInodeChangeDate': u'2024:07:01 12:55:11-04:00', u'EXE:UninitializedDataSize': 1024, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.4.0.0'}]
Mime Type	application/x-dosexec
Imphash	3abe302b6d9a1256e6a915429af4ffd2

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6068	0x6200	6.45071390001	adb3e7aaafcc05f64701b4c2f6385889
.rdata	0x8000	0x1250	0x1400	5.04163613318	99b48cddaa99007d1d87676aa49e9798
.data	0xa000	0x399058	0x400	5.13238478013	f95027c0eac5eb0bf708aa96757ff20d
.ndata	0x3a4000	0x22000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rsrc	0x3c6000	0x5aa90	0x5ac00	4.19454712875	0a944c5002d43e43a46e4c5a49f345c6

PE Imports

- KERNEL32.dll
  - GetTempPathA
  - GetFileSize
  - GetModuleFileNameA
  - GetCurrentProcess
  - CopyFileA
  - ExitProcess
  - SetEnvironmentVariableA
  - Sleep
  - GetTickCount
  - GetCommandLineA
  - lstrlenA
  - GetVersion
  - SetErrorMode
  - lstrcpynA
  - GetDiskFreeSpaceA
  - GlobalUnlock
  - GetWindowsDirectoryA
  - SetCurrentDirectoryA
  - GetLastError
  - CreateDirectoryA
  - CreateProcessA
  - RemoveDirectoryA
  - CreateFileA
  - GetTempFileNameA
  - ReadFile
  - WriteFile
  - lstrcpyA
  - MoveFileExA
  - lstrcatA
  - GetSystemDirectoryA
  - GetProcAddress
  - GetExitCodeProcess
  - WaitForSingleObject
  - CompareFileTime
  - SetFileAttributesA
  - GetFileAttributesA
  - GetShortPathNameA
  - MoveFileA
  - GetFullPathNameA
  - SetFileTime
  - SearchPathA
  - CloseHandle
  - lstrcmpiA
  - CreateThread
  - GlobalLock
  - lstrcmpA
  - FindFirstFileA
  - FindNextFileA
  - DeleteFileA
  - SetFilePointer
  - GetPrivateProfileStringA
  - FindClose
  - MultiByteToWideChar
  - FreeLibrary
  - MulDiv
  - WritePrivateProfileStringA
  - LoadLibraryExA
  - GetModuleHandleA

    - GlobalAlloc
    - GlobalFree
    - ExpandEnvironmentStringsA
- USER32.dll
    - ScreenToClient
    - GetSystemMenu
    - SetClassLongA
    - IsWindowEnabled
    - SetWindowPos
    - GetSysColor
    - GetWindowLongA
    - SetCursor
    - LoadCursorA
    - CheckDlgButton
    - GetMessagePos
    - LoadBitmapA
    - CallWindowProcA
    - IsWindowVisible
    - CloseClipboard
    - SetClipboardData
    - EmptyClipboard
    - PostQuitMessage
    - GetWindowRect
    - EnableMenuItem
    - CreatePopupMenu
    - GetSystemMetrics
    - SetDlgItemTextA
    - GetDlgItemTextA
    - MessageBoxIndirectA
    - CharPrevA
    - DispatchMessageA
    - PeekMessageA
    - ReleaseDC
    - EnableWindow
    - InvalidateRect
    - SendMessageA
    - DefWindowProcA
    - BeginPaint
    - GetClientRect
    - FillRect
    - DrawTextA
    - EndDialog
    - RegisterClassA
    - SystemParametersInfoA
    - CreateWindowExA
    - GetClassInfoA
    - DialogBoxParamA
    - CharNextA
    - ExitWindowsEx
    - GetDC
    - CreateDialogParamA
    - SetTimer
    - GetDlgItem
    - SetWindowLongA
    - SetForegroundWindow
    - LoadImageA
    - IsWindow
    - SendMessageTimeoutA
    - FindWindowExA
    - OpenClipboard
    - TrackPopupMenu
    - AppendMenuA
    - EndPaint
    - DestroyWindow
    - wsprintfA
    - ShowWindow
    - SetWindowTextA
- GDI32.dll
    - SelectObject
    - SetBkMode
    - CreateFontIndirectA
    - SetTextColor
    - DeleteObject
    - GetDeviceCaps
    - CreateBrushIndirect

- SetBkColor
- SHELL32.dll
  - SHGetSpecialFolderLocation
  - ShellExecuteExA
  - SHGetPathFromIDListA
  - SHBrowseForFolderA
  - SHGetFileInfoA
  - SHFileOperationA
- ADVAPI32.dll
  - AdjustTokenPrivileges
  - RegCreateKeyExA
  - RegOpenKeyExA
  - SetFileSecurityA
  - OpenProcessToken
  - LookupPrivilegeValueA
  - RegEnumValueA
  - RegDeleteKeyA
  - RegDeleteValueA
  - RegCloseKey
  - RegSetValueExA
  - RegQueryValueExA
  - RegEnumKeyA
- COMCTL32.dll
  - ImageList_Create
  - ImageList_AddMasked
  - ImageList_Destroy
  - None
- ole32.dll
  - OleUninitialize
  - OleInitialize
  - CoTaskMemFree
  - CoCreateInstance

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 3957880, u'sha256': u'914ae123d2b230484ccb8a351d99b50aff024b059c7e5e869da5b89e1400ed0d', u'type': u'dBase IV DBT, blocks size 0, block length 8192, next free block index 40, next free block 0, next used block 0', u'size': 270376}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4228256, u'sha256': u'd9433a671e0eea301a770be87e5de4c2b4fb82a323666d62478a1172b4b2f9d5', u'type': u'dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0', u'size': 67624}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4295880, u'sha256': u'd7e075d9fe4ba866051ea6355a1e14aaabd8fa5a170ebfe1002f52254a7f0651', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4305520, u'sha256': u'e9686cd6662c0b0af0823ac90709019b150b50a1b9d71e7da25f1880dde69ca4', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4309784, u'sha256': u'07003ce26d8f946b66ccae27ffca7a5934c3d1d6e5482152643340eb9ac4eb5c', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4313536, u'sha256': u'86414c758e75d62cbb8fb82732ed52909cab7ce51694d3e99cfc5c7be59395ba', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4315976, u'sha256': u'1c19529795a20280233b7ba76e8631c46b727ddf580fba91e2adb28f9a6c6856', u'type': u'dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 16579055, next used block 16118770', u'size': 2216}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4318192, u'sha256': u'1bac4541a38451ec6f7000e2d62d3fe9c848a23fa2f894140eac4f6613be01f2', u'type': u'data', u'size': 1736}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4319928, u'sha256': u'150625c5e665ec395fffd85dd05ab74e1ffb61438182644f37904f5cdd4c05cb', u'type': u'data', u'size': 1640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4321568, u'sha256': u'935d8426085866fdbd878b79f86feb94b04d01174cc3290df1571dd7281e6958', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4322952, u'sha256': u'd9b652e38446e2c937190aac259214fb80fc7ada2c4bae48186989a57bb9eeed', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4324080, u'sha256': u'fcf930459a81913f64b4a5f06187ebeda88c6355eaac532aec7760dc2e5851ad', u'type': u'dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2298019839, next used block 128', u'size': 744}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4324824, u'sha256': u'da2408936dbd0c1f976f45fb67d41207ca6fbb329c859d84d3dd2db4d6f9bc6a', u'type': u'data', u'size': 488}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 4325312, u'sha256': u'63682e6cf4b81efa2a17b2a1f39ed3613a0745c536e0b695c78f118dc0144de9', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 296}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 4325608, u'sha256': u'fecdb955f8d7f1c219ff8167f90b64f3cb52e53337494577ff73c0ac1dafcd96', u'type': u'data', u'size': 256}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 4325864, u'sha256': u'69897c784f1491eb3024b0d52c2897196a2e245974497fda1915db5fefcf8729', u'type': u'data', u'size': 284}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 4326152, u'sha256':

u'2d986f26ff752607366192a903078cdd7d6da06ab97309c85cd5c8cf05f823b6', u'type': u'data', u'size': 196}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 4326352, u'sha256': u'85025c8556952f6a651c2468c8a0d58853b0ba482be9ad5cd3060f216540dfc0', u'type': u'data', u'size': 96}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 4326448, u'sha256': u'c2e09563484e00a6e450554128ff00bf104768216ef9c936e89fe7acb6f0bf5a', u'type': u'MS Windows icon resource - 14 icons, 48x48, 16 colors', u'size': 202}

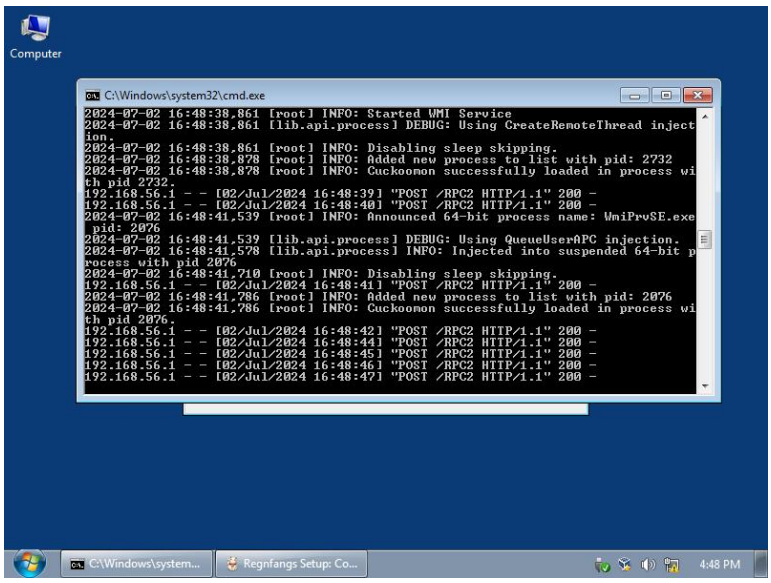
{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 4326656, u'sha256': u'e2ca706c975c96edeaad16d662cf64d361d0ad120b3cfa268c75bc92b3c3a101', u'type': u'data', u'size': 356}

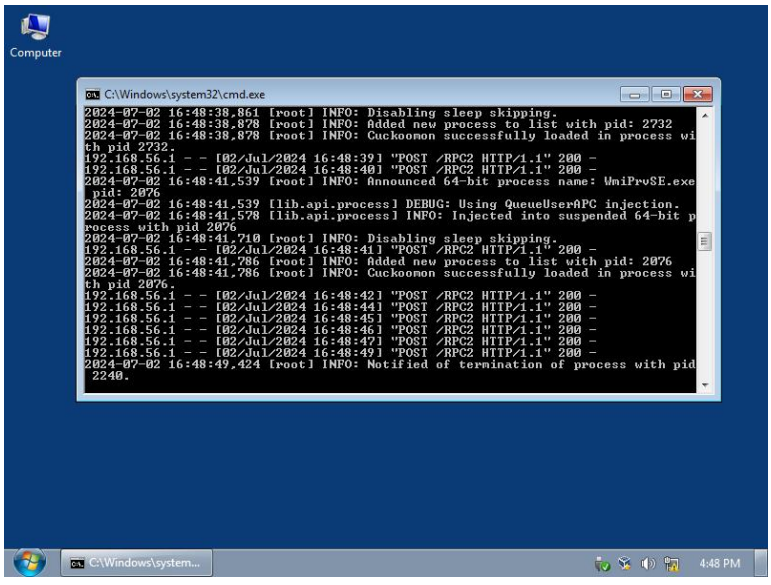
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 4327016, u'sha256': u'e40393270907 39a6754db86ef1704a8a07115ceb11719c0987a9d00a77a77f16', u'type': u'XML 1.0 document, ASCII text, with very long lines, with no line terminators', u'size': 1059}

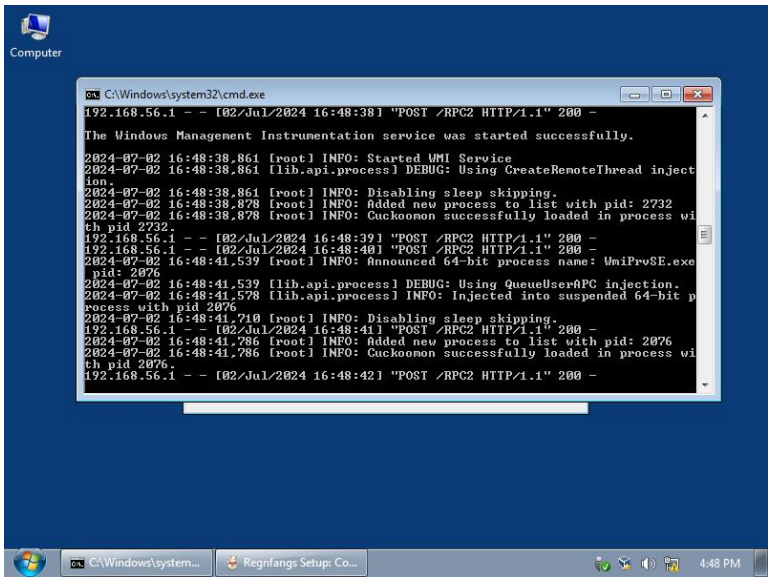
CERTIFICATE VALIDATION

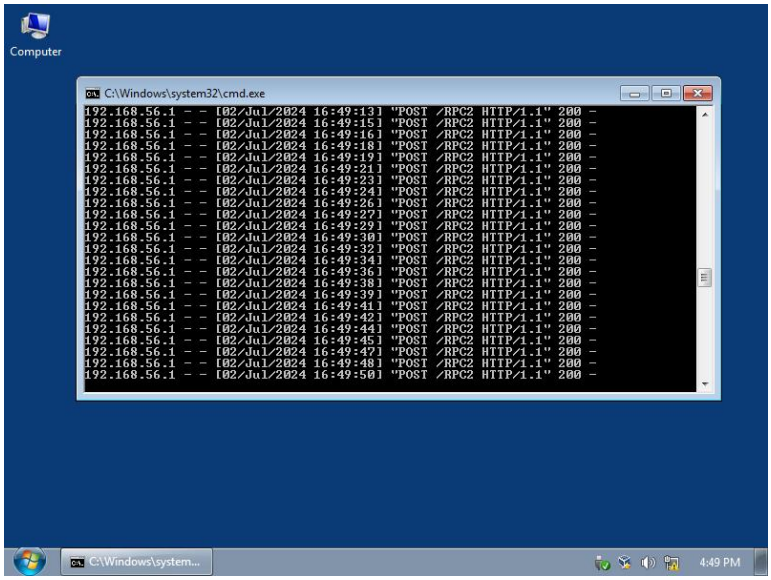
- Certificate Validation is not Applicable ?

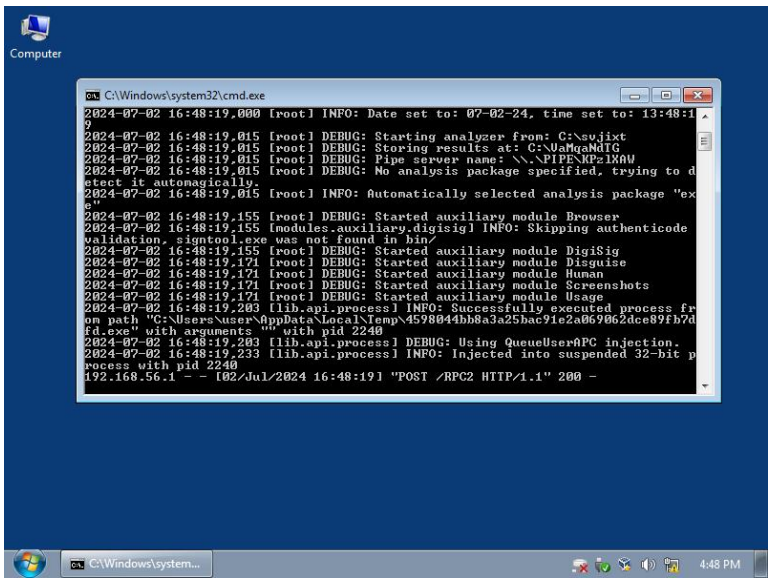
SCREENSHOTS

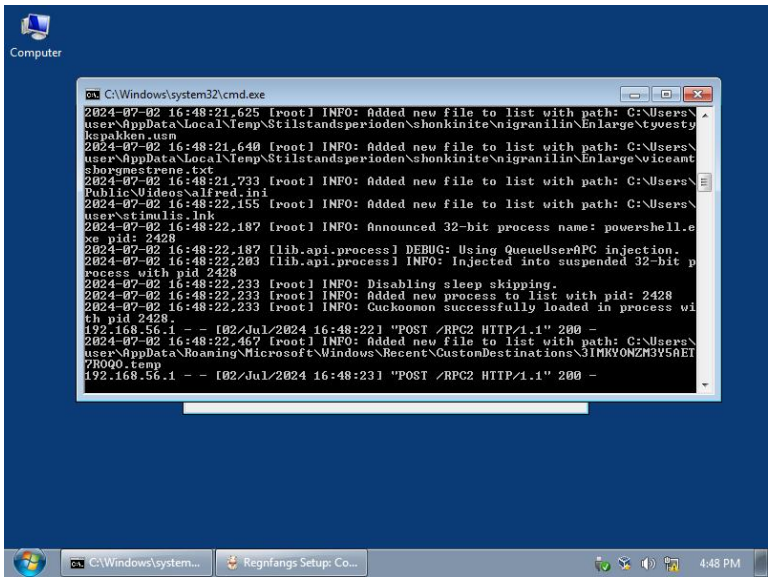


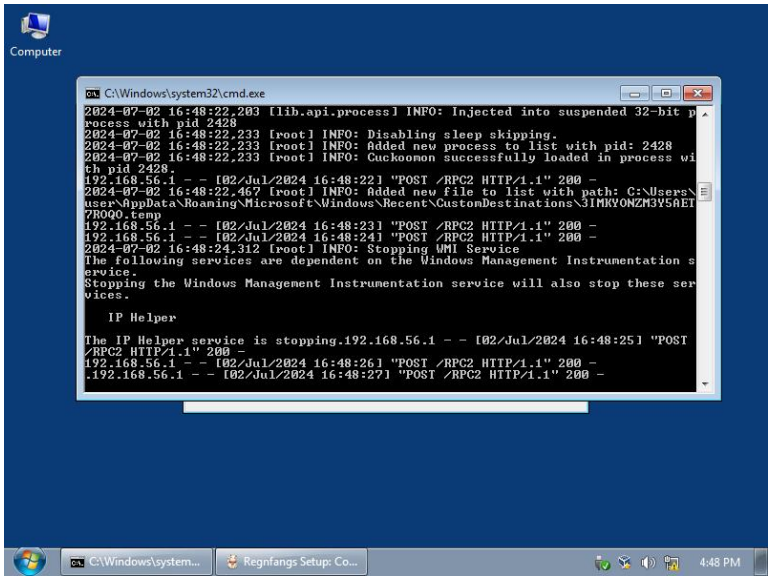


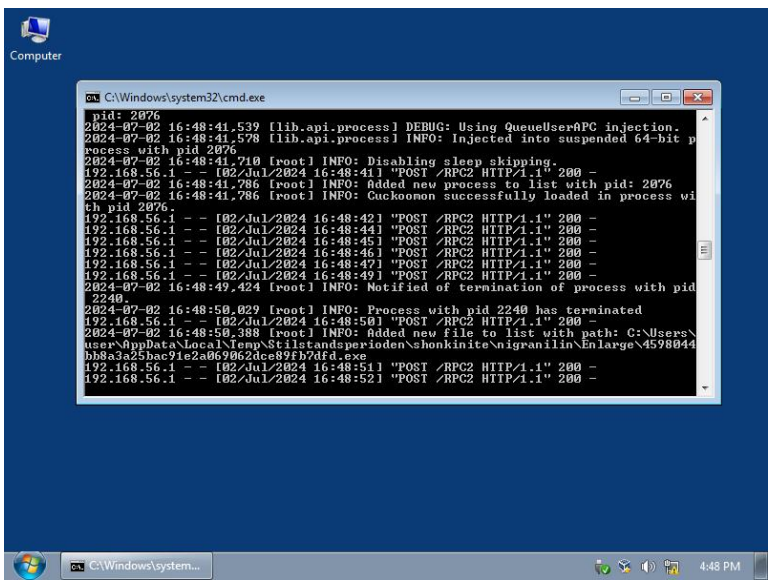

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:38] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-07-02 16:48:38,861 [root] INFO: Started WMI Service
2024-07-02 16:48:38,861 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-07-02 16:48:38,861 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:38,878 [root] INFO: Added new process to list with pid: 2732
2024-07-02 16:48:38,878 [root] INFO: Cuckoomon successfully loaded in process with pid 2732.
192.168.56.1 - - [02/Jul/2024 16:48:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:40] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,539 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2076
2024-07-02 16:48:41,539 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:41,578 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2076
2024-07-02 16:48:41,710 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [02/Jul/2024 16:48:41] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process with pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

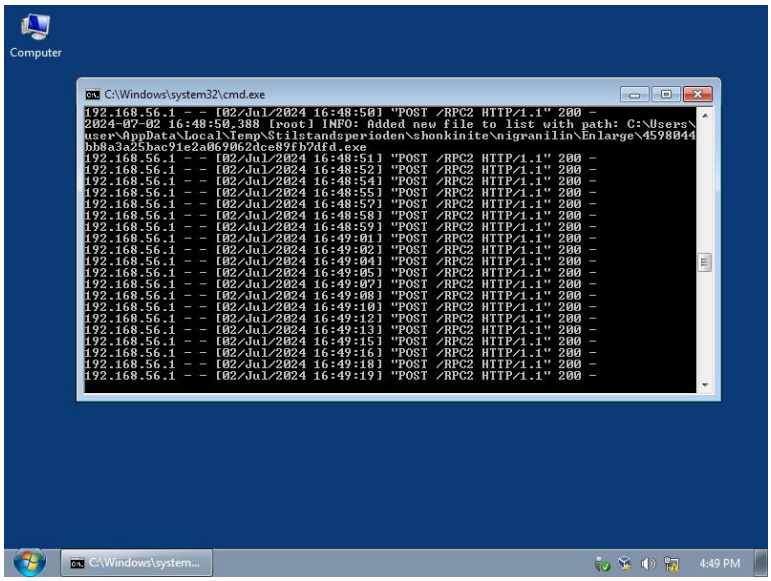

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:50] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

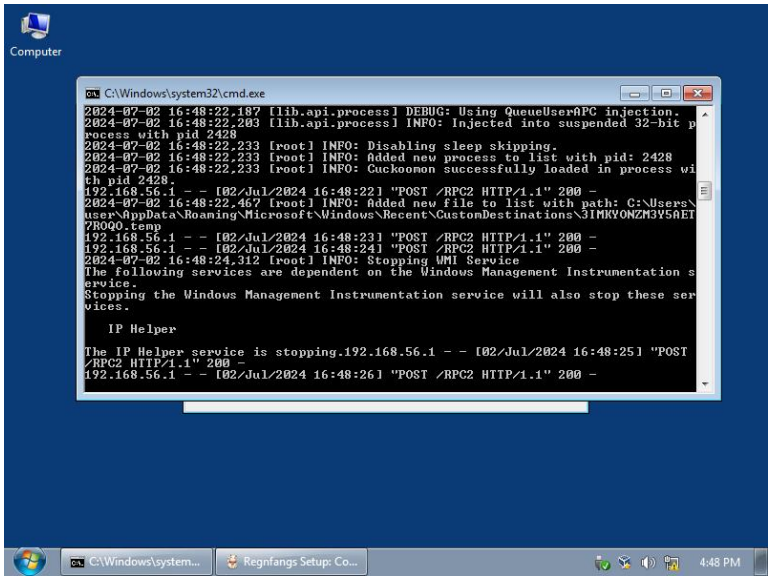

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:19,000 [root] INFO: Date set to: 07-02-24, time set to: 13:48:19
2024-07-02 16:48:19,015 [root] DEBUG: Starting analyzer from: C:\svjixt
2024-07-02 16:48:19,015 [root] DEBUG: Storing results at: C:\VaMqaNdTG
2024-07-02 16:48:19,015 [root] DEBUG: Pipe server name: \\.\PIPE\KPz1XAW
2024-07-02 16:48:19,015 [root] DEBUG: No analysis package specified, trying to detect it automagically.
2024-07-02 16:48:19,015 [root] INFO: Automatically selected analysis package "exe"
2024-07-02 16:48:19,155 [root] DEBUG: Started auxiliary module Browser
2024-07-02 16:48:19,155 [modules.auxiliary.digisig] INFO: Skipping authenticode validation, signtool.exe was not found in bin/
2024-07-02 16:48:19,155 [root] DEBUG: Started auxiliary module DigiSig
2024-07-02 16:48:19,171 [root] DEBUG: Started auxiliary module Disguise
2024-07-02 16:48:19,171 [root] DEBUG: Started auxiliary module Human
2024-07-02 16:48:19,171 [root] DEBUG: Started auxiliary module Screenshots
2024-07-02 16:48:19,171 [root] DEBUG: Started auxiliary module Usage
2024-07-02 16:48:19,203 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe" with arguments "" with pid 2240
2024-07-02 16:48:19,203 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:19,233 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2240
192.168.56.1 - - [02/Jul/2024 16:48:19] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:48 PM

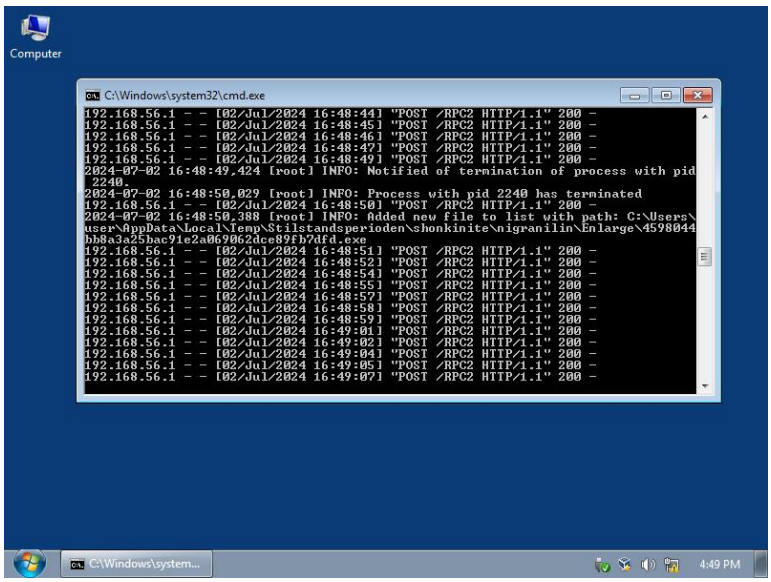

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:21,625 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\tyvestykspakken.usn
2024-07-02 16:48:21,640 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\viceamtsborgmestrene.txt
2024-07-02 16:48:21,733 [root] INFO: Added new file to list with path: C:\Users\Public\Videos\alFred.ini
2024-07-02 16:48:22,155 [root] INFO: Added new file to list with path: C:\Users\user\stimulis.lnk
2024-07-02 16:48:22,187 [root] INFO: Announced 32-bit process name: powershell.exe pid: 2428
2024-07-02 16:48:22,187 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:22,203 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2428
2024-07-02 16:48:22,233 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:22,233 [root] INFO: Added new process to list with pid: 2428
2024-07-02 16:48:22,233 [root] INFO: Cuckoomon successfully loaded in process with pid 2428.
192.168.56.1 - - [02/Jul/2024 16:48:22] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:22,467 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3IMKYONZM3Y5AET7ROQO.temp
192.168.56.1 - - [02/Jul/2024 16:48:23] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

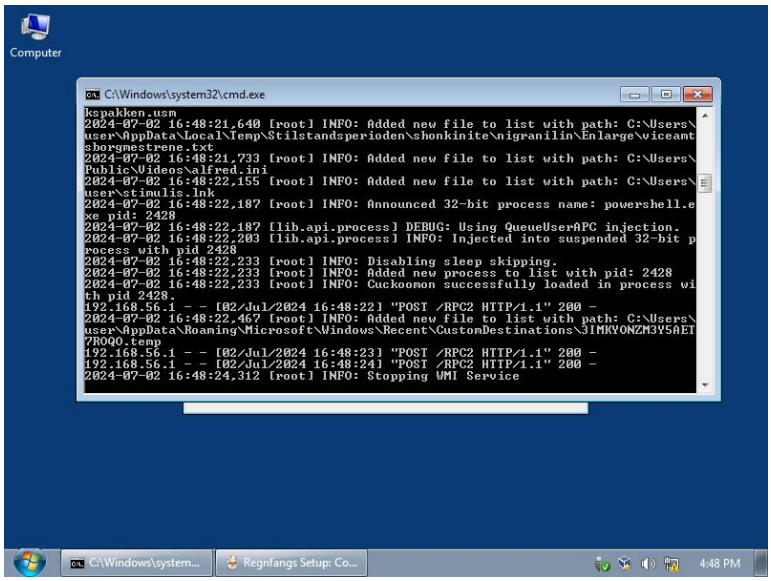

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:22,203 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2428
2024-07-02 16:48:22,233 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:22,233 [root] INFO: Added new process to list with pid: 2428
2024-07-02 16:48:22,233 [root] INFO: Cuckoomon successfully loaded in process with pid 2428.
192.168.56.1 - - [02/Jul/2024 16:48:22] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:22,467 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3IMKYONZM3Y5AET7ROQO.temp
192.168.56.1 - - [02/Jul/2024 16:48:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:24] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:24,312 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.
IP Helper
The IP Helper service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:27] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

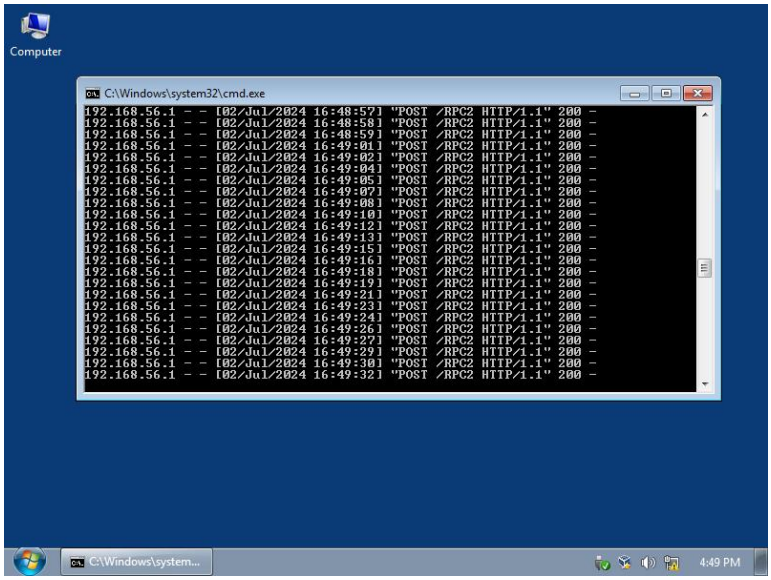

Computer
C:\Windows\system32\cmd.exe
pid: 2076
2024-07-02 16:48:41,539 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:41,570 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2076
2024-07-02 16:48:41,710 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [02/Jul/2024 16:48:41] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process with pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid 2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:48 PM

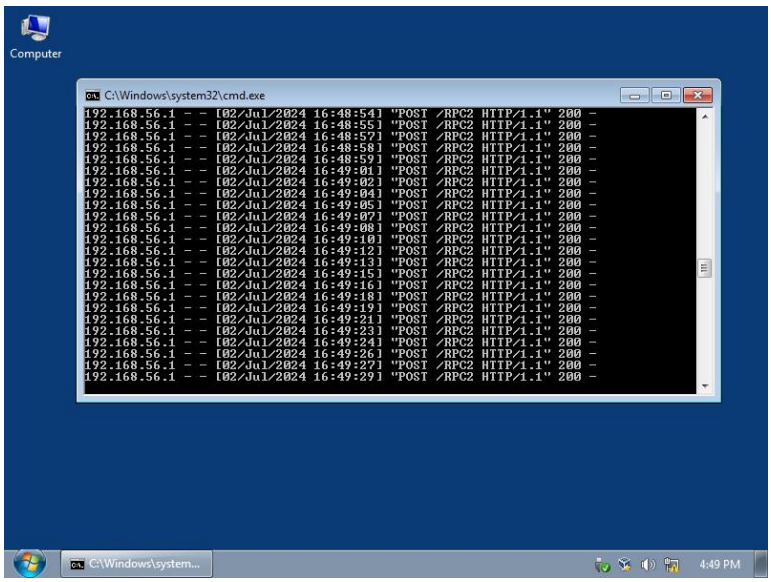

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

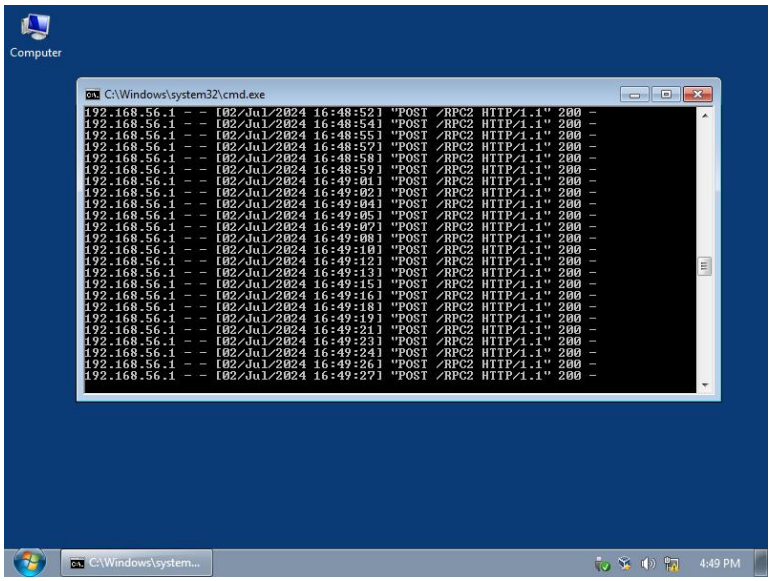

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:22,187 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:22,203 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2428
2024-07-02 16:48:22,233 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:22,233 [root] INFO: Added new process to list with pid: 2428
2024-07-02 16:48:22,233 [root] INFO: Cuckoomon successfully loaded in process with pid 2428.
192.168.56.1 - - [02/Jul/2024 16:48:22] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:22,467 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3IMKYONZM3Y5AET7ROQO.temp
192.168.56.1 - - [02/Jul/2024 16:48:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:24] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:24,312 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.
IP Helper
The IP Helper service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:26] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

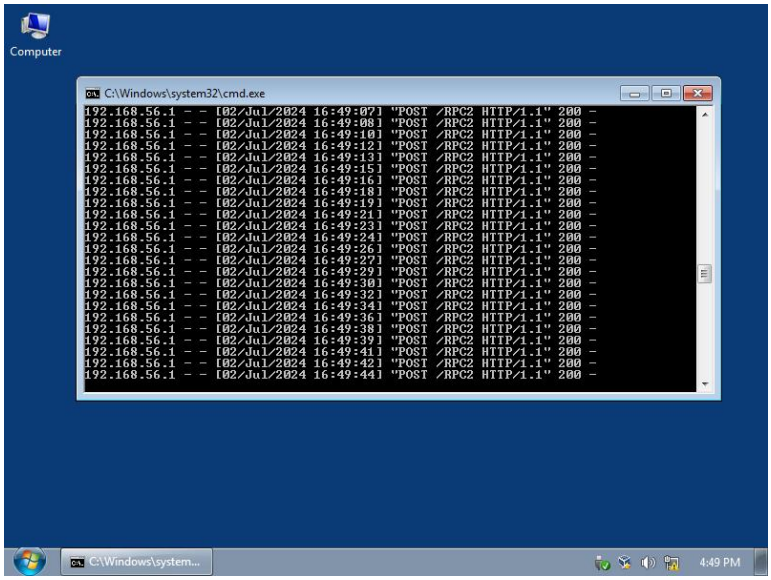

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid 2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

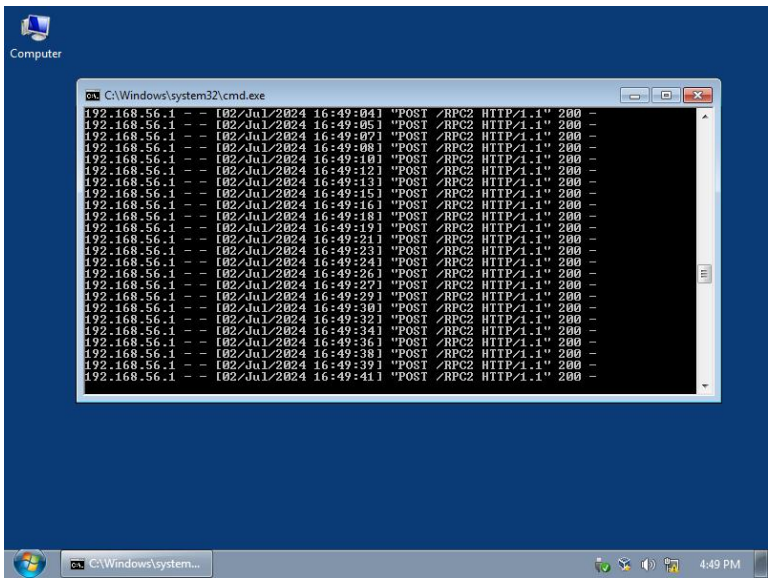

Computer
C:\Windows\system32\cmd.exe
kspakken.usm
2024-07-02 16:48:21,640 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\viceamtsborgmestrene.txt
2024-07-02 16:48:21,733 [root] INFO: Added new file to list with path: C:\Users\Public\Videos\alfred.ini
2024-07-02 16:48:22,155 [root] INFO: Added new file to list with path: C:\Users\user\stimulis.lnk
2024-07-02 16:48:22,187 [root] INFO: Announced 32-bit process name: powershell.exe pid: 2428
2024-07-02 16:48:22,187 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:22,203 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2428
2024-07-02 16:48:22,233 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:22,233 [root] INFO: Added new process to list with pid: 2428
2024-07-02 16:48:22,233 [root] INFO: Cuckoomon successfully loaded in process with pid 2428.
192.168.56.1 - - [02/Jul/2024 16:48:22] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:22,467 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3IMKYONZM3Y5AEI7ROQO.temp
192.168.56.1 - - [02/Jul/2024 16:48:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:24] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:24,312 [root] INFO: Stopping WMI Service
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

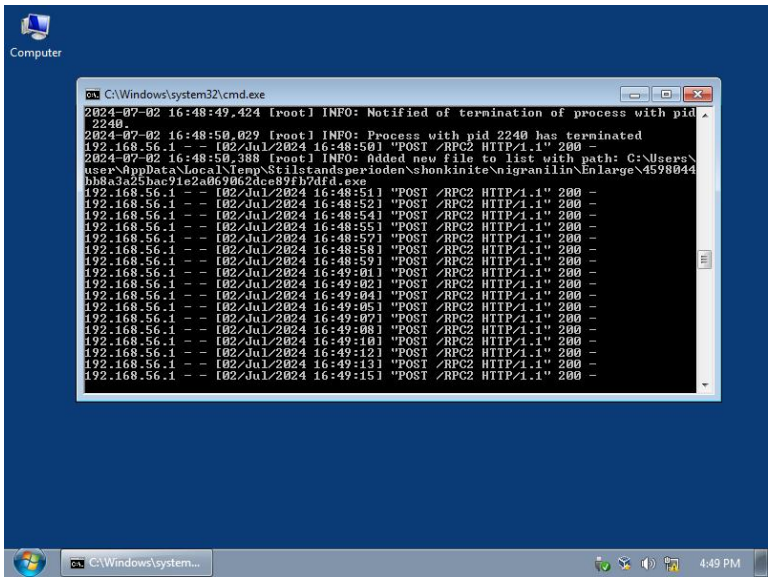

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

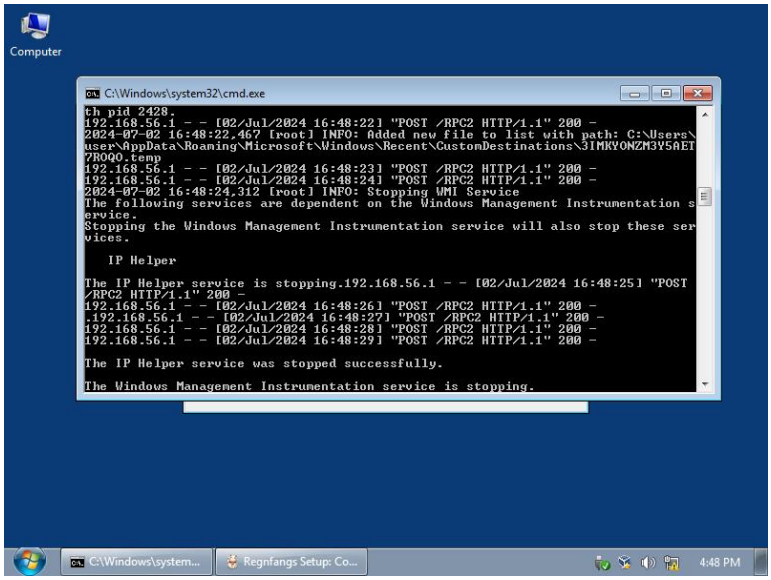

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

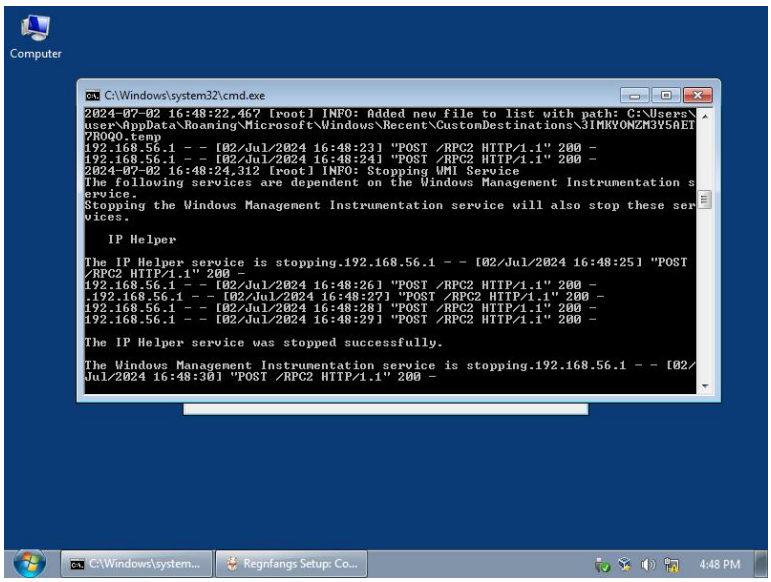

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

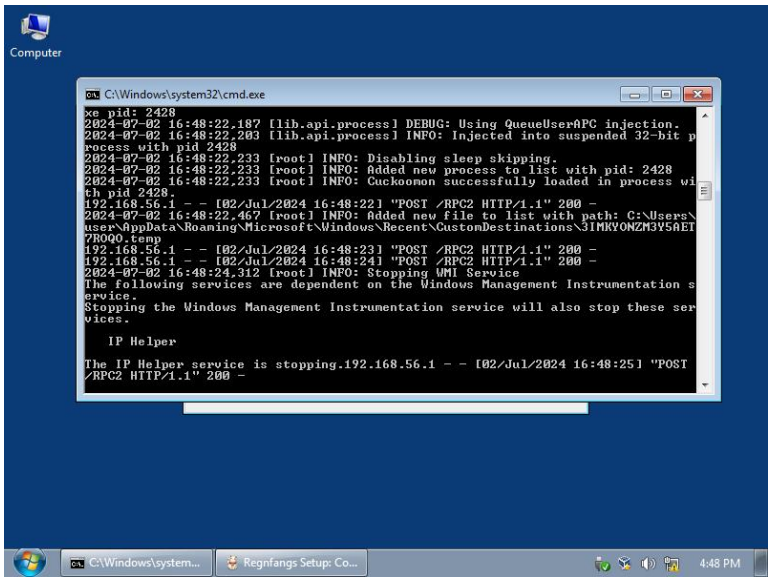

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:44] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

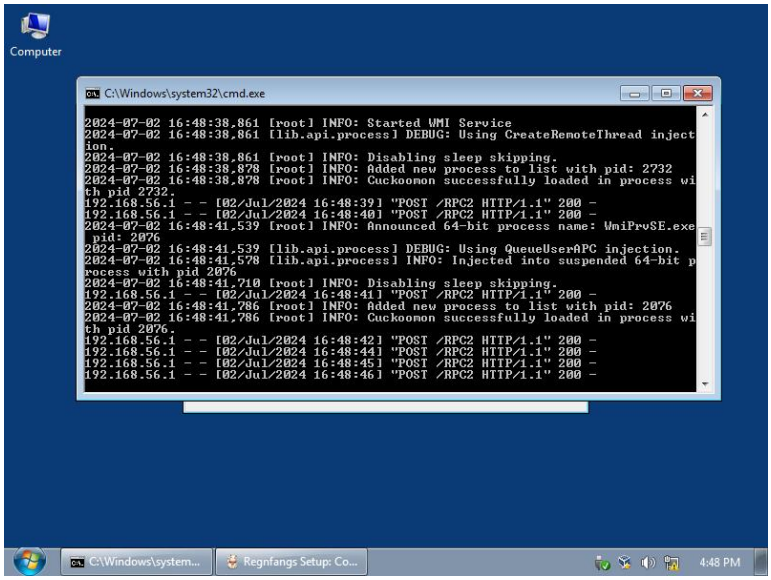

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:41] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

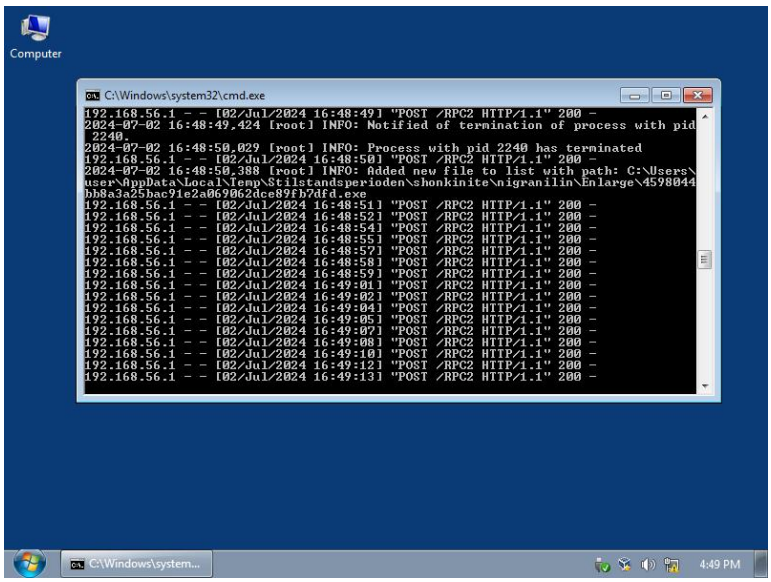

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid 2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

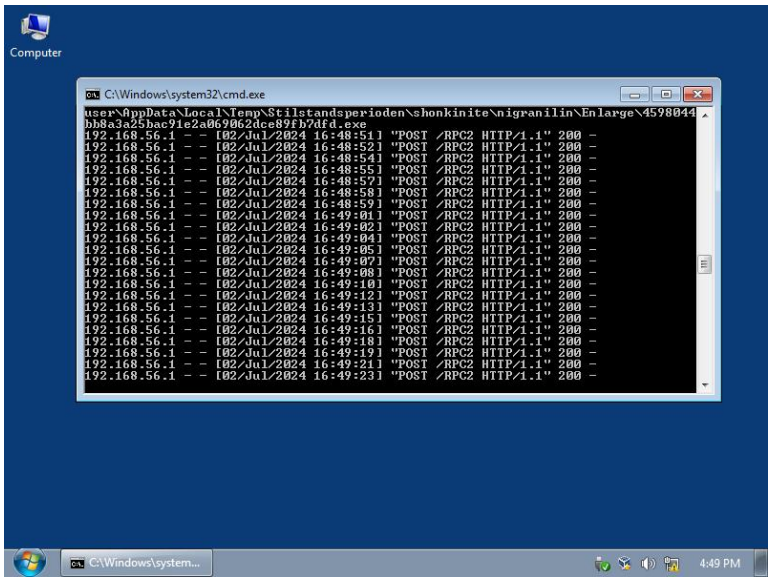

Computer
C:\Windows\system32\cmd.exe
th pid 2428.
192.168.56.1 - - [02/Jul/2024 16:48:22] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:22,467 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3IMKYONZM3Y5AET7ROQO.temp
192.168.56.1 - - [02/Jul/2024 16:48:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:24] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:24,312 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.
IP Helper
The IP Helper service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:29] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

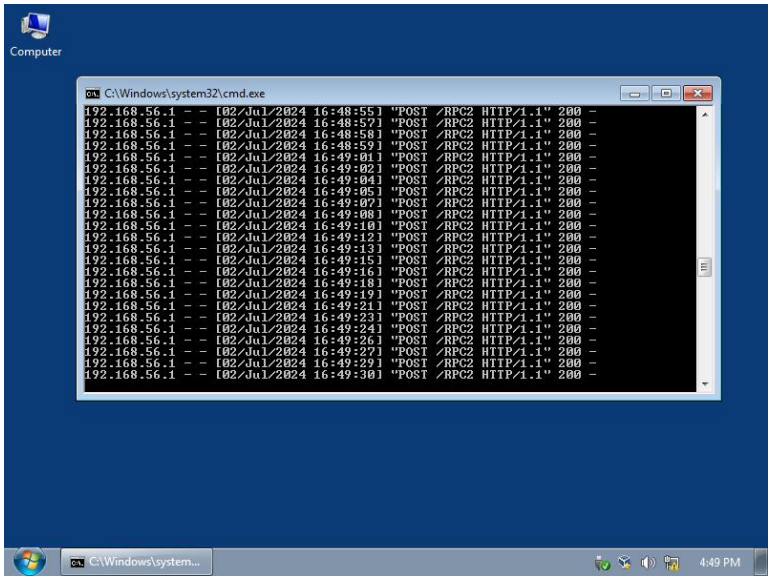

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:22,467 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3IMKYONZM3Y5AET7ROQO.temp
192.168.56.1 - - [02/Jul/2024 16:48:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:24] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:24,312 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.
IP Helper
The IP Helper service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:29] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:30] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

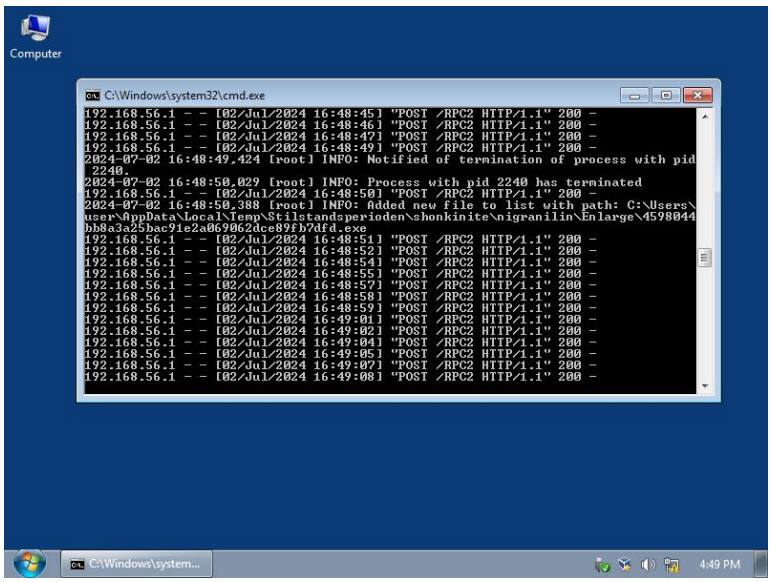

Computer
C:\Windows\system32\cmd.exe
xe pid: 2428
2024-07-02 16:48:22,187 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:22,203 [lib.api.process] INFO: Injected into suspended 32-bit p
rocess with pid 2428
2024-07-02 16:48:22,233 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:22,233 [root] INFO: Added new process to list with pid: 2428
2024-07-02 16:48:22,233 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2428.
192.168.56.1 - - [02/Jul/2024 16:48:22] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:22,467 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3IMKYONZM3Y5AET
7ROQO.temp
192.168.56.1 - - [02/Jul/2024 16:48:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:24] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:24,312 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation s
ervice.
Stopping the Windows Management Instrumentation service will also stop these ser
vices.
IP Helper
The IP Helper service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:25] "POST
/RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

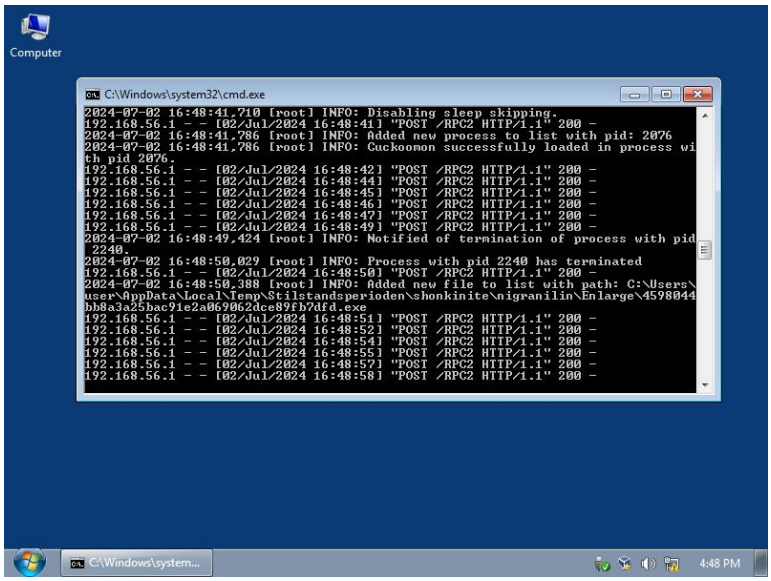

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:38,861 [root] INFO: Started WMI Service
2024-07-02 16:48:38,861 [lib.api.process] DEBUG: Using CreateRemoteThread inject
ion.
2024-07-02 16:48:38,861 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:38,878 [root] INFO: Added new process to list with pid: 2732
2024-07-02 16:48:38,878 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2732.
192.168.56.1 - - [02/Jul/2024 16:48:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:40] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,539 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe
pid: 2076
2024-07-02 16:48:41,539 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:41,570 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2076
2024-07-02 16:48:41,710 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [02/Jul/2024 16:48:41] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

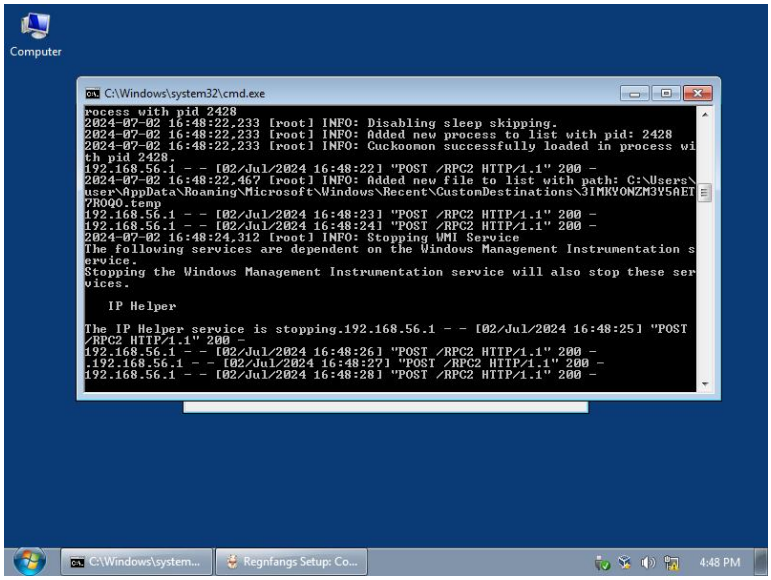

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid
2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044
bb8a3a25bac91e2a069062dca89f17dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

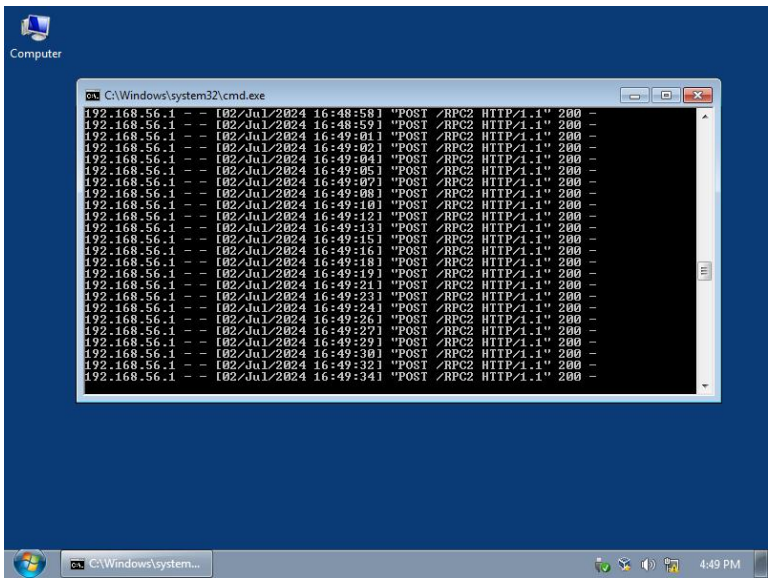

Computer
C:\Windows\system32\cmd.exe
user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044
bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

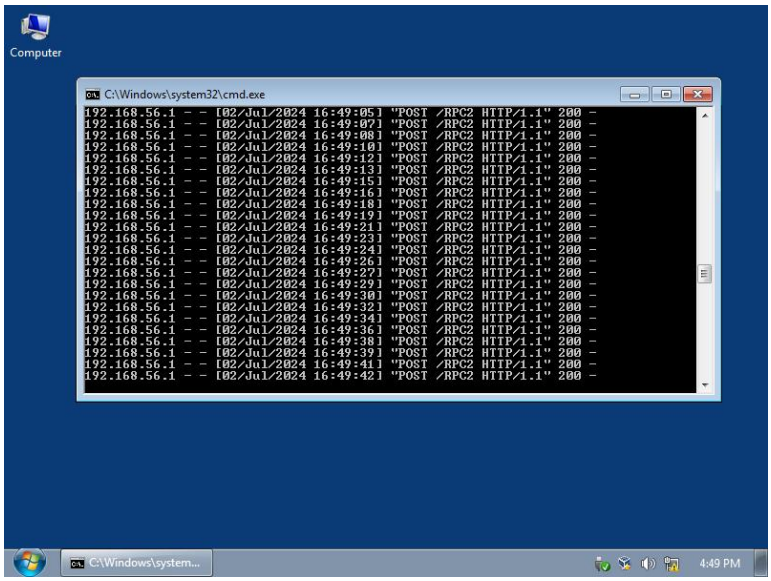

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

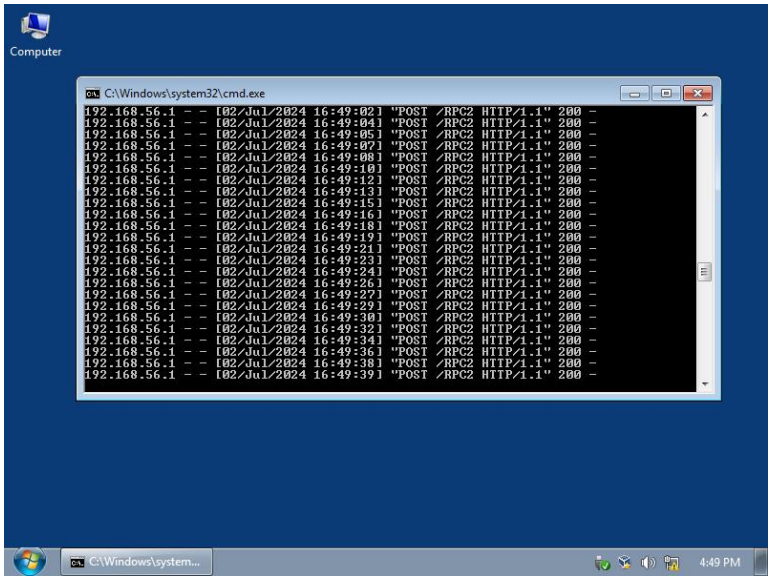

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49.424 [root] INFO: Notified of termination of process with pid
2240.
2024-07-02 16:48:50.029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50.388 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044
bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

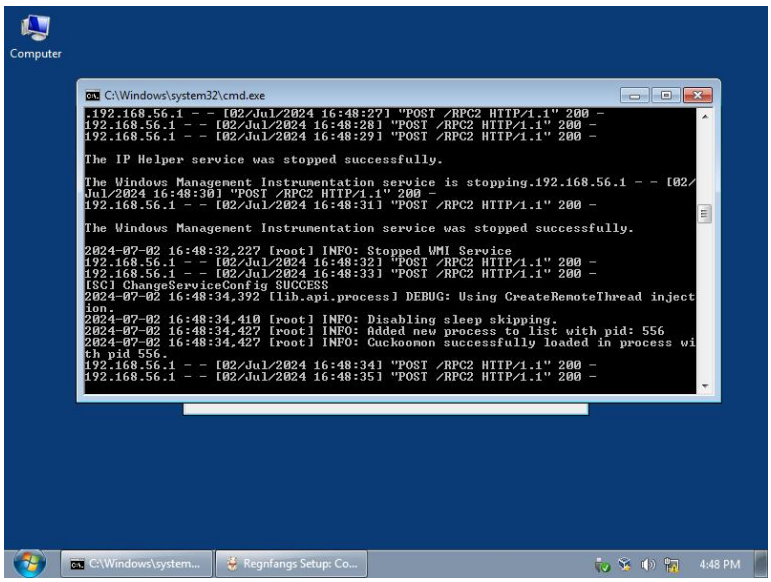

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:41,710 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [02/Jul/2024 16:48:41] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process with pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid 2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:48 PM

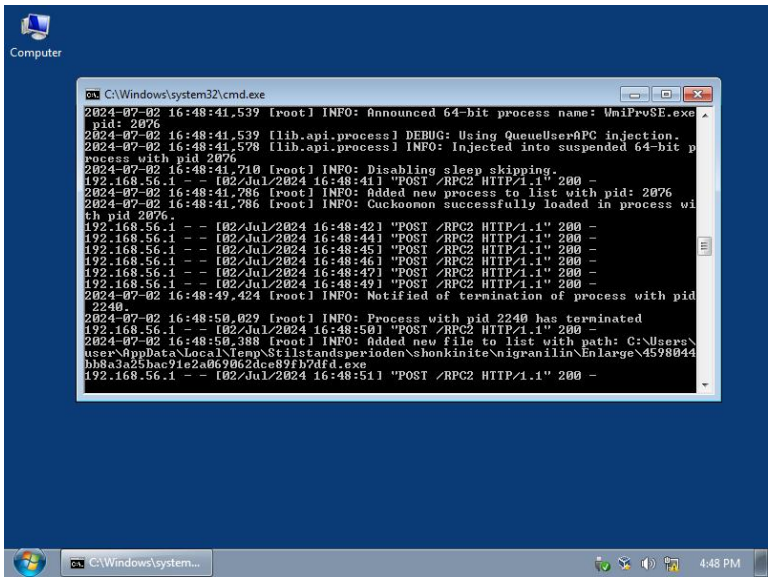

Computer
C:\Windows\system32\cmd.exe
rocess with pid 2428
2024-07-02 16:48:22,233 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:22,233 [root] INFO: Added new process to list with pid: 2428
2024-07-02 16:48:22,233 [root] INFO: Cuckoomon successfully loaded in process with pid 2428.
192.168.56.1 - - [02/Jul/2024 16:48:22] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:22,467 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3IMXYONZM3Y5AEI7BOQO.temp
192.168.56.1 - - [02/Jul/2024 16:48:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:24] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:24,312 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.
IP Helper
The IP Helper service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:26] "POST /RPC2 HTTP/1.1" 200 -
.192.168.56.1 - - [02/Jul/2024 16:48:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:28] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

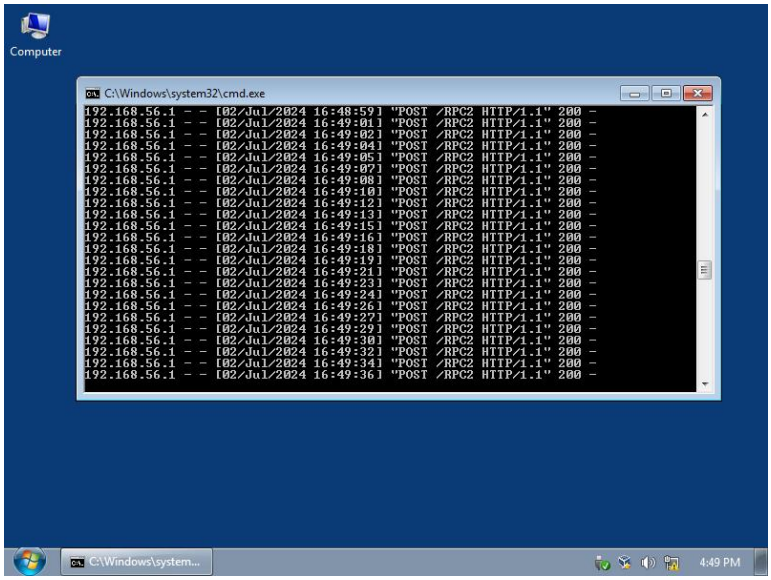

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:34] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

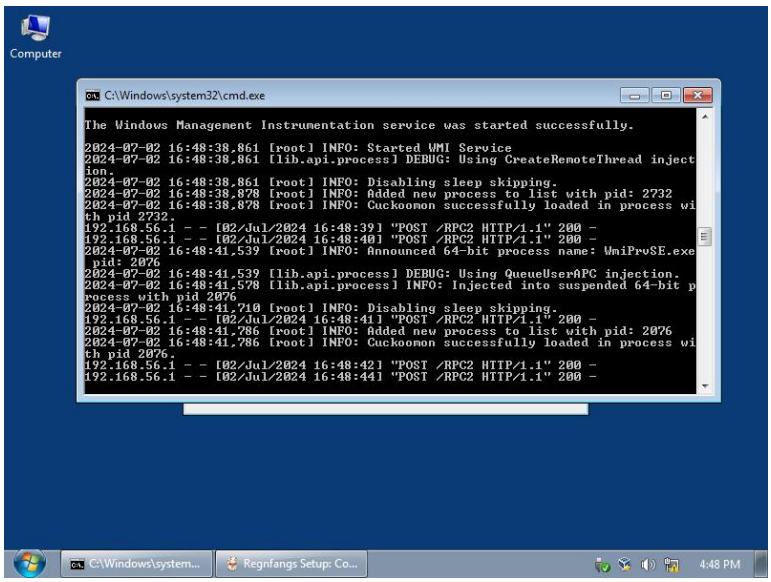

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:42] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

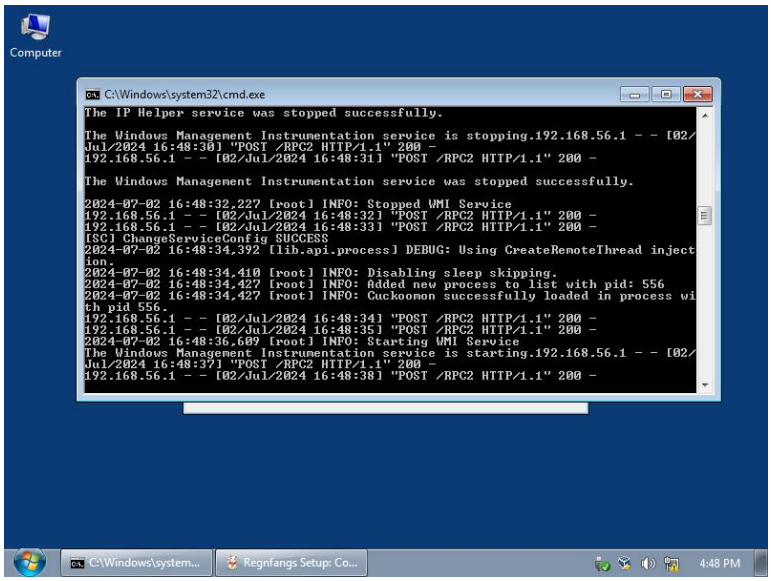

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:39] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

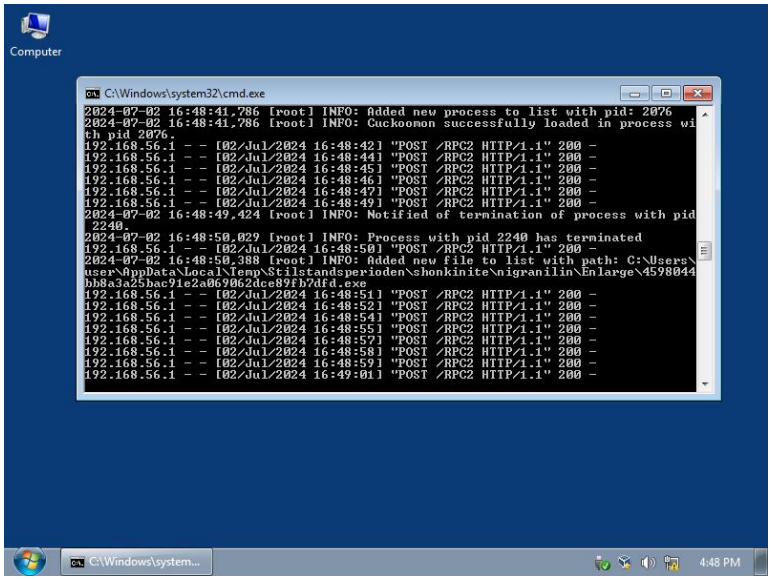

Computer
C:\Windows\system32\cmd.exe
.192.168.56.1 - - [02/Jul/2024 16:48:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:29] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [02/
Jul/2024 16:48:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:31] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was stopped successfully.
2024-07-02 16:48:32.227 [root] INFO: Stopped WMI Service
192.168.56.1 - - [02/Jul/2024 16:48:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:33] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-07-02 16:48:34.392 [lib.api.process] DEBUG: Using CreateRemoteThread inject
ion.
2024-07-02 16:48:34.410 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:34.427 [root] INFO: Added new process to list with pid: 556
2024-07-02 16:48:34.427 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 556.
192.168.56.1 - - [02/Jul/2024 16:48:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:35] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

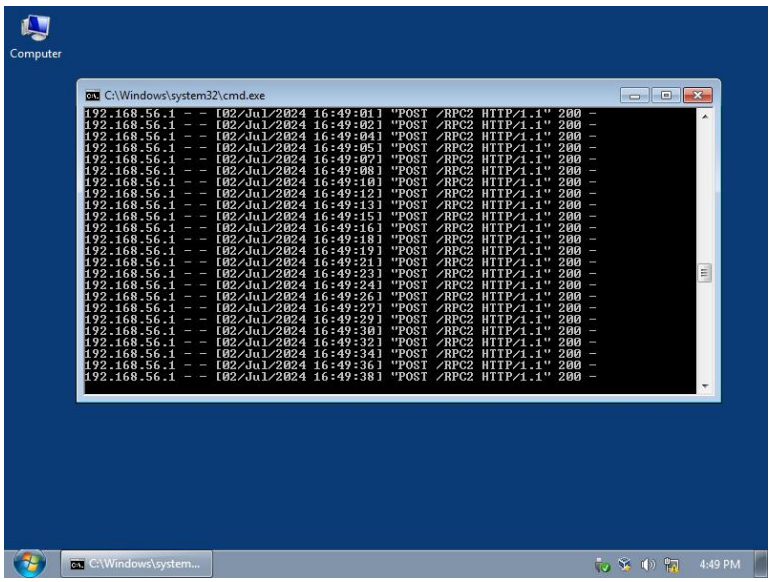

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:41,539 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2076
2024-07-02 16:48:41,539 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:41,578 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2076
2024-07-02 16:48:41,710 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [02/Jul/2024 16:48:41] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process with pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid 2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:48 PM

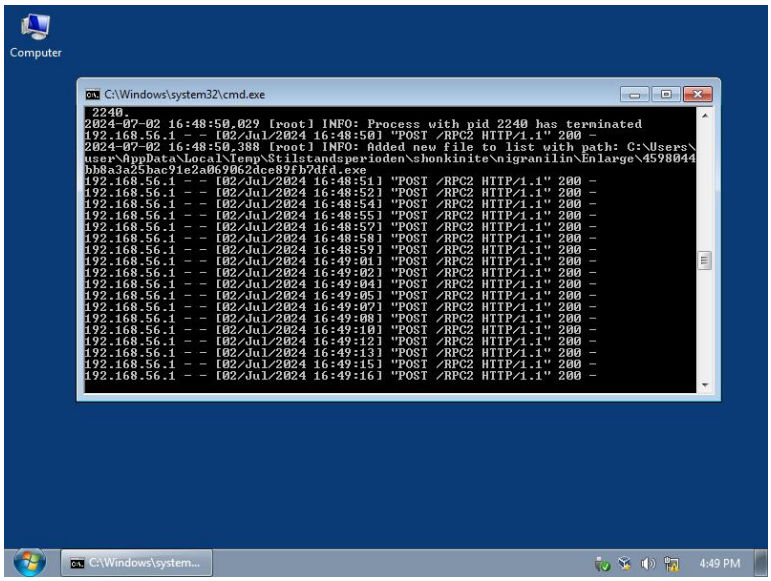

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:36] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

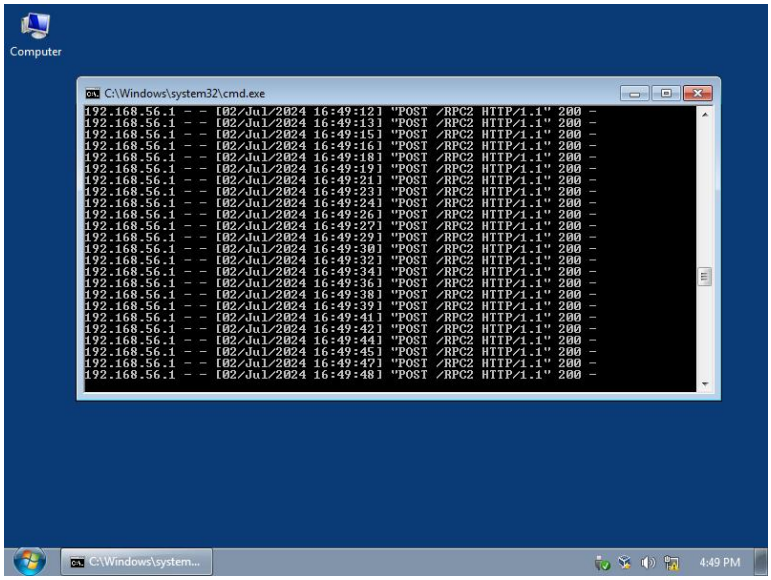

Computer
C:\Windows\system32\cmd.exe
The Windows Management Instrumentation service was started successfully.
2024-07-02 16:48:38,861 [root] INFO: Started WMI Service
2024-07-02 16:48:38,861 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-07-02 16:48:38,861 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:38,878 [root] INFO: Added new process to list with pid: 2732
2024-07-02 16:48:38,878 [root] INFO: Cuckoomon successfully loaded in process with pid 2732.
192.168.56.1 - - [02/Jul/2024 16:48:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:40] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,539 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2076
2024-07-02 16:48:41,539 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:41,578 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2076
2024-07-02 16:48:41,710 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [02/Jul/2024 16:48:41] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process with pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

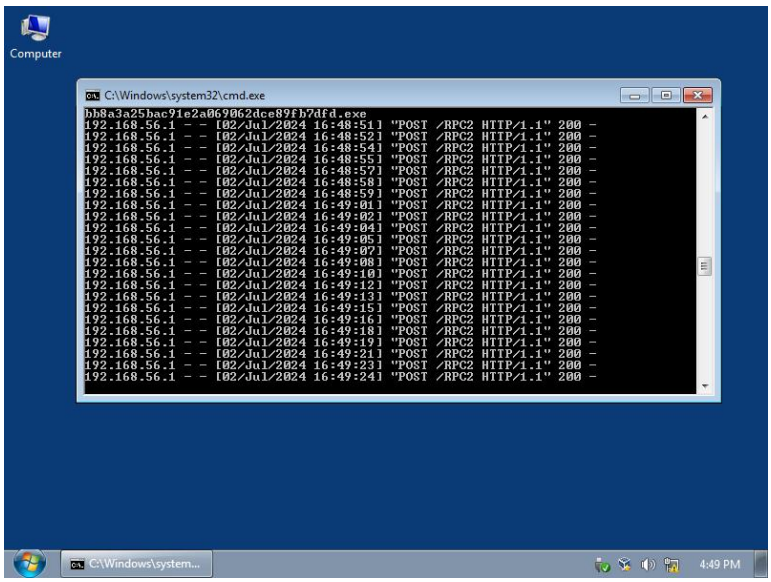

Computer
C:\Windows\system32\cmd.exe
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:31] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was stopped successfully.
2024-07-02 16:48:32,227 [root] INFO: Stopped WMI Service
192.168.56.1 - - [02/Jul/2024 16:48:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:33] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-07-02 16:48:34,392 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-07-02 16:48:34,410 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:34,427 [root] INFO: Added new process to list with pid: 556
2024-07-02 16:48:34,427 [root] INFO: Cuckoomon successfully loaded in process with pid 556.
192.168.56.1 - - [02/Jul/2024 16:48:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:35] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:36,609 [root] INFO: Starting WMI Service
The Windows Management Instrumentation service is starting.192.168.56.1 - - [02/Jul/2024 16:48:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:38] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

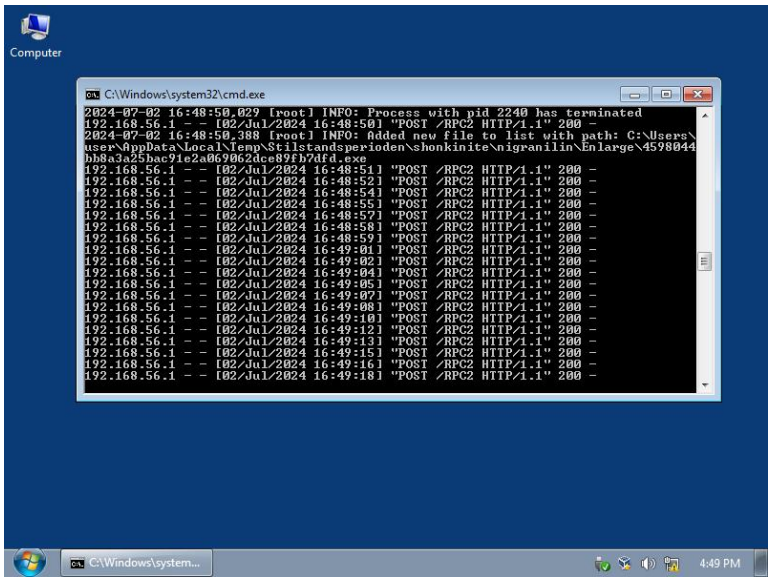

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process with pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid 2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:48 PM

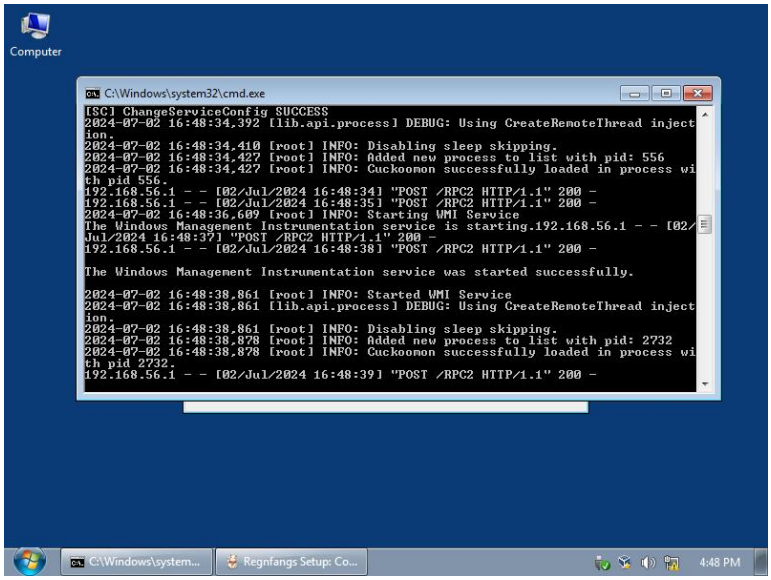

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:38] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

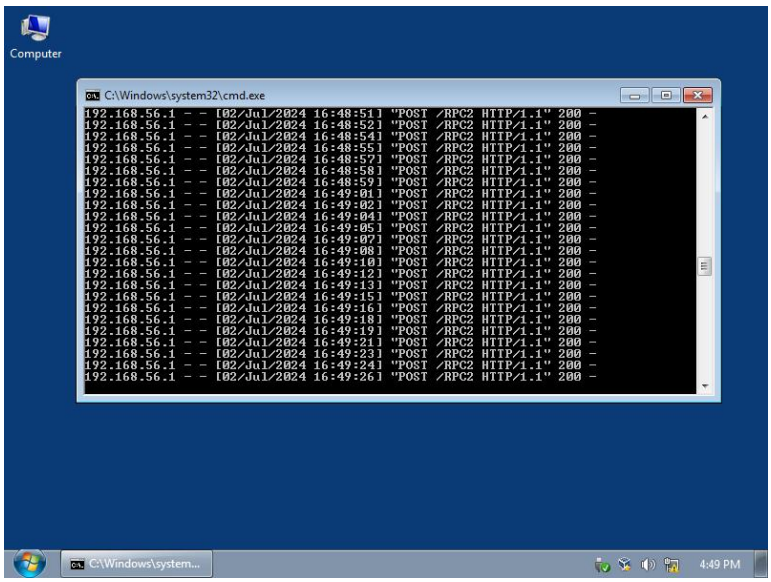

Computer
C:\Windows\system32\cmd.exe
2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

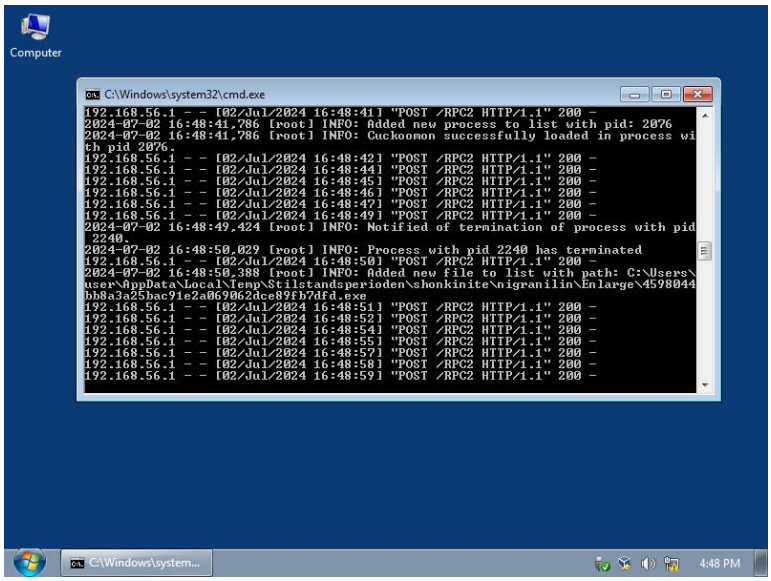

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:48] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

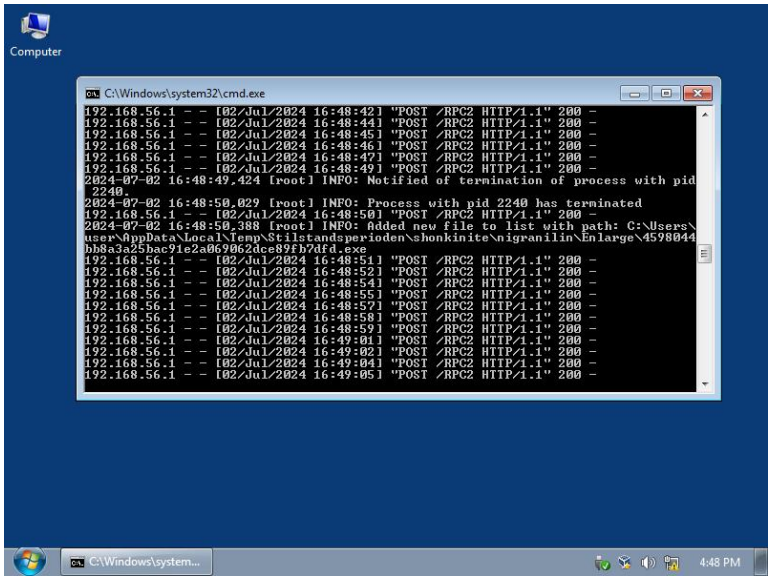

Computer
C:\Windows\system32\cmd.exe
bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

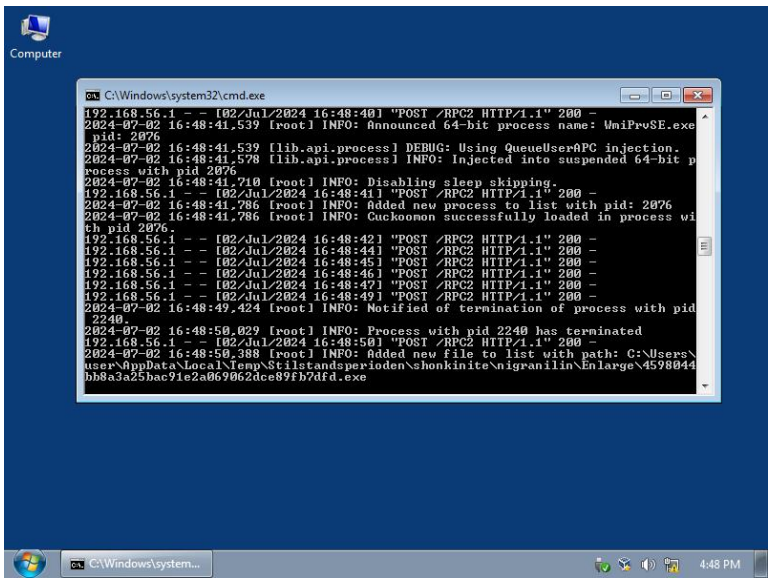

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,380 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

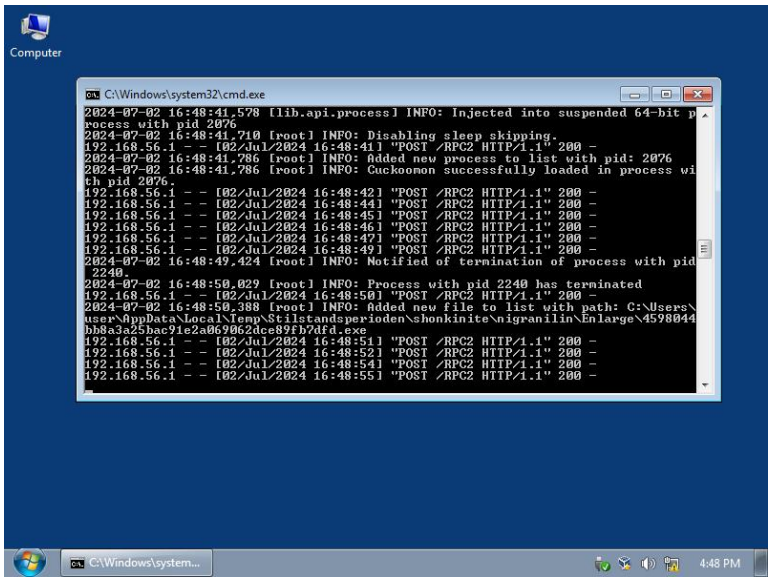

Computer
C:\Windows\system32\cmd.exe
[SC] ChangeServiceConfig SUCCESS
2024-07-02 16:48:34,392 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-07-02 16:48:34,410 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:34,427 [root] INFO: Added new process to list with pid: 556
2024-07-02 16:48:34,427 [root] INFO: Cuckoomon successfully loaded in process with pid 556.
192.168.56.1 - - [02/Jul/2024 16:48:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:35] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:36,609 [root] INFO: Starting WMI Service
The Windows Management Instrumentation service is starting.192.168.56.1 - - [02/Jul/2024 16:48:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:38] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-07-02 16:48:38,861 [root] INFO: Started WMI Service
2024-07-02 16:48:38,861 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-07-02 16:48:38,861 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:38,878 [root] INFO: Added new process to list with pid: 2732
2024-07-02 16:48:38,878 [root] INFO: Cuckoomon successfully loaded in process with pid 2732.
192.168.56.1 - - [02/Jul/2024 16:48:39] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

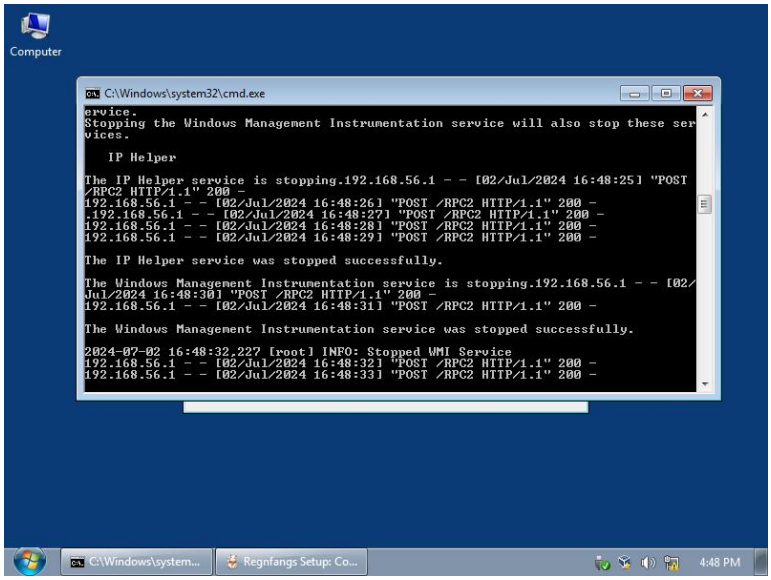

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

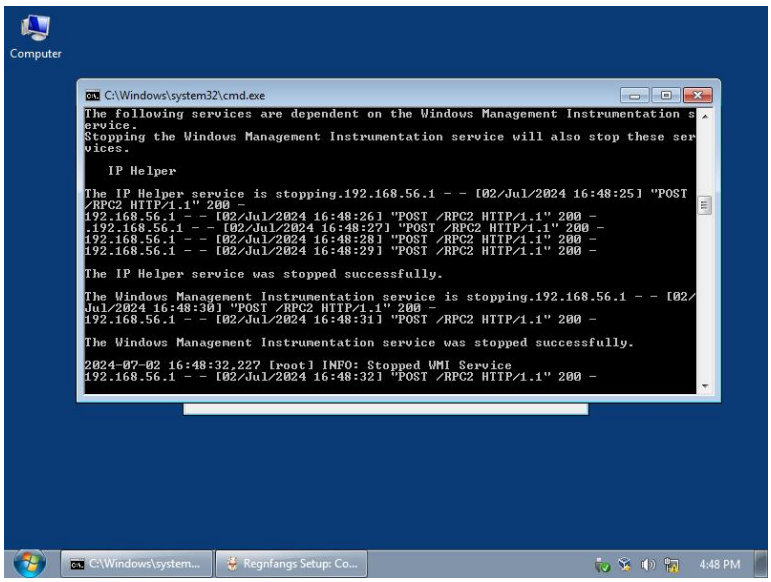

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:41] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process with pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid 2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:48 PM

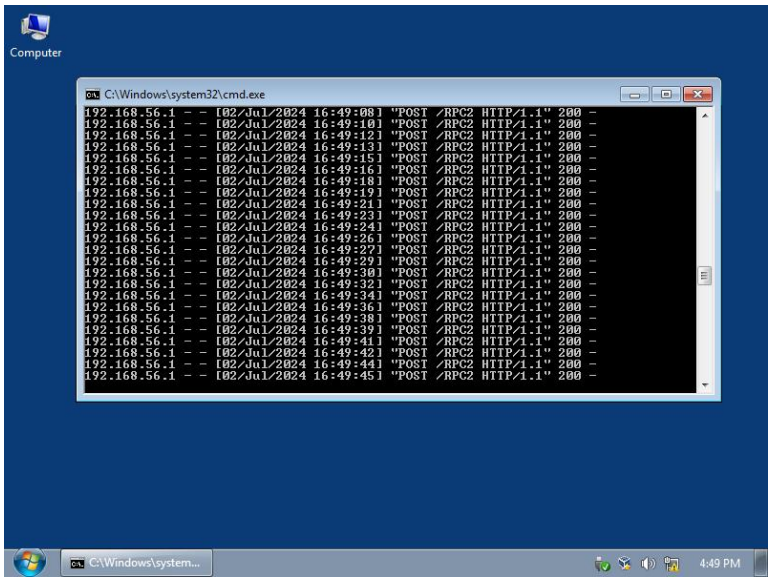

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid 2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:48 PM

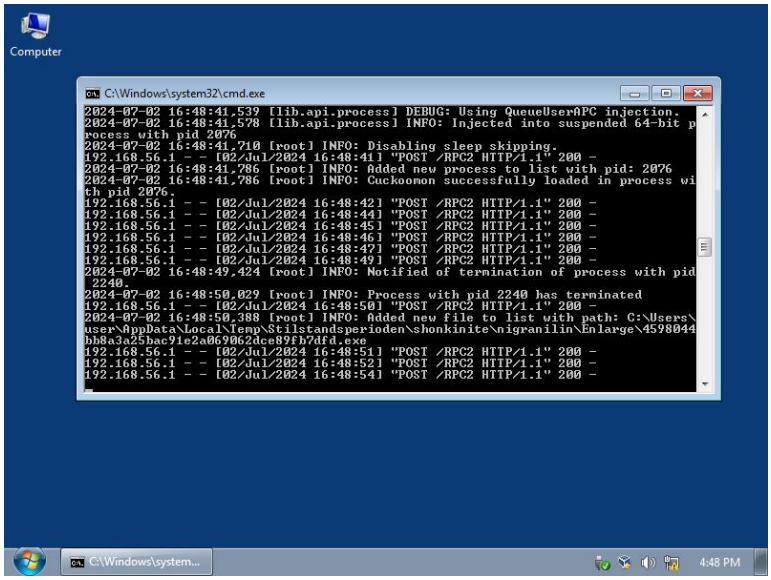

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:40] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,539 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2076
2024-07-02 16:48:41,539 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:41,578 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2076
2024-07-02 16:48:41,710 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [02/Jul/2024 16:48:41] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process with pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid 2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
C:\Windows\system...
4:48 PM

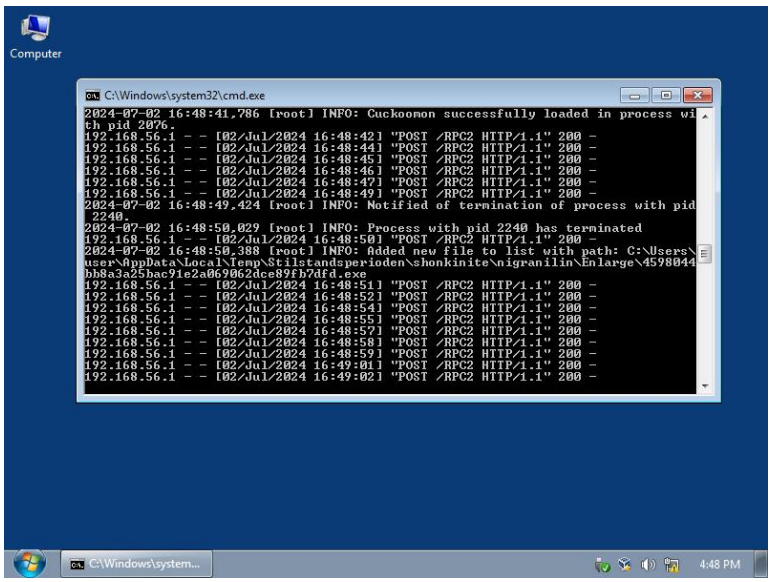

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:41,578 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2076
2024-07-02 16:48:41,710 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [02/Jul/2024 16:48:41] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process with pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid 2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:48 PM

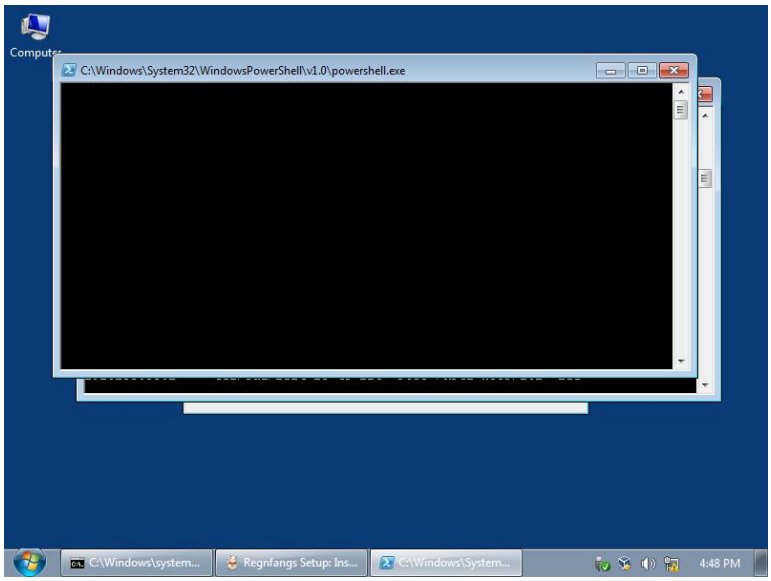

Computer
C:\Windows\system32\cmd.exe
ervice.
Stopping the Windows Management Instrumentation service will also stop these services.
IP Helper
The IP Helper service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:26] "POST /RPC2 HTTP/1.1" 200 -
.192.168.56.1 - - [02/Jul/2024 16:48:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:29] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:31] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was stopped successfully.
2024-07-02 16:48:32,227 [root] INFO: Stopped WMI Service
192.168.56.1 - - [02/Jul/2024 16:48:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:33] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

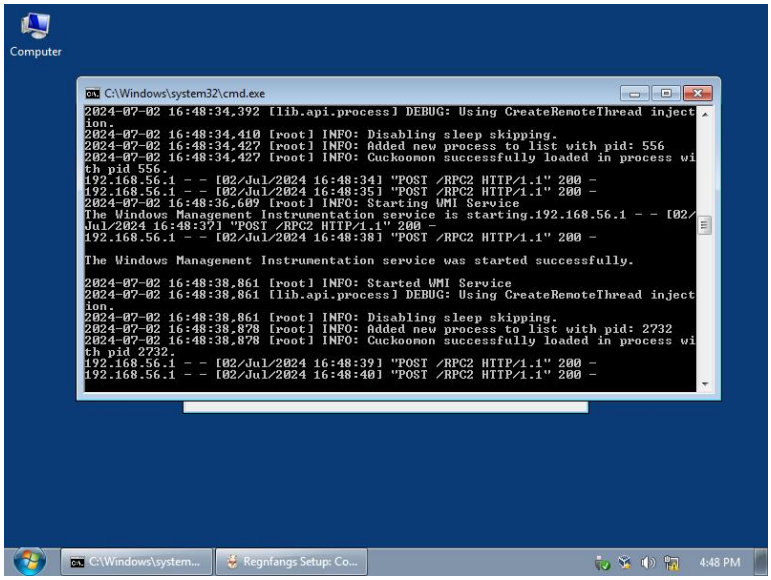

Computer
C:\Windows\system32\cmd.exe
The following services are dependent on the Windows Management Instrumentation service.
Stopping the Windows Management Instrumentation service will also stop these services.
IP Helper
The IP Helper service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:25] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:26] "POST /RPC2 HTTP/1.1" 200 -
.192.168.56.1 - - [02/Jul/2024 16:48:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:29] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:31] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was stopped successfully.
2024-07-02 16:48:32,227 [root] INFO: Stopped WMI Service
192.168.56.1 - - [02/Jul/2024 16:48:32] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

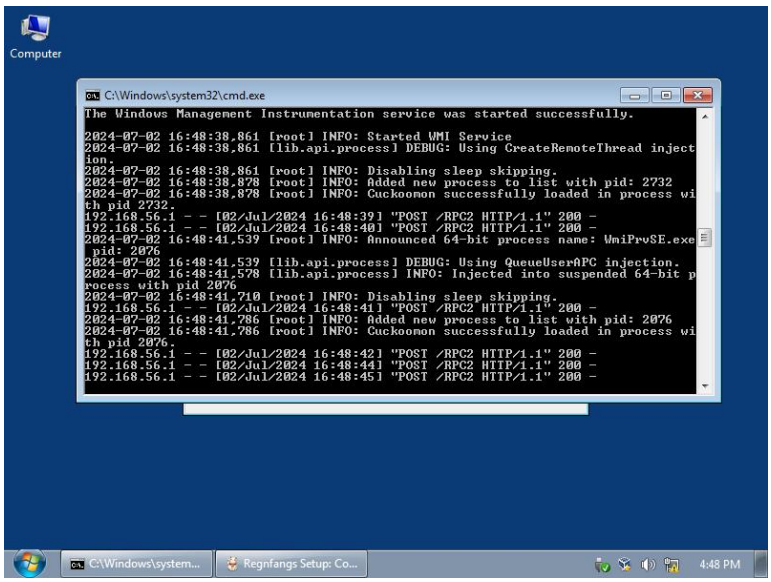

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:45] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

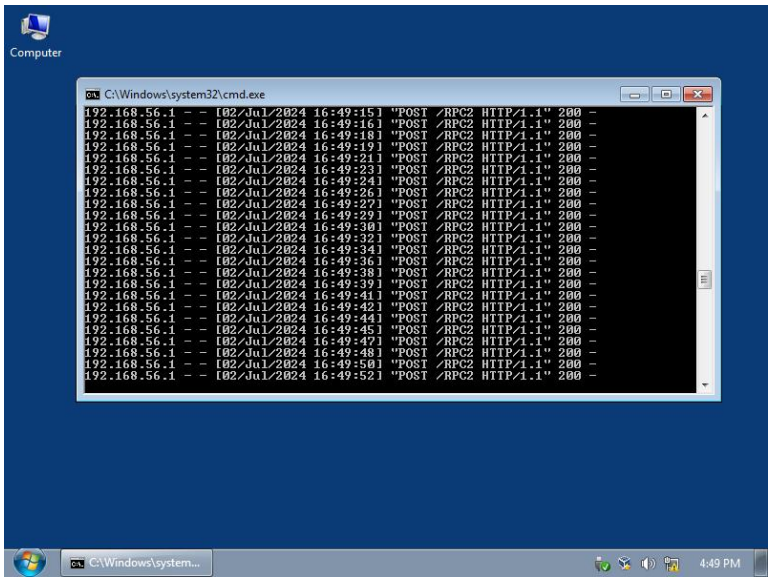

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:41,539 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:41,578 [lib.api.process] INFO: Injected into suspended 64-bit p
rocess with pid 2076.
2024-07-02 16:48:41,710 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [02/Jul/2024 16:48:41] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid
2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044
bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:48 PM

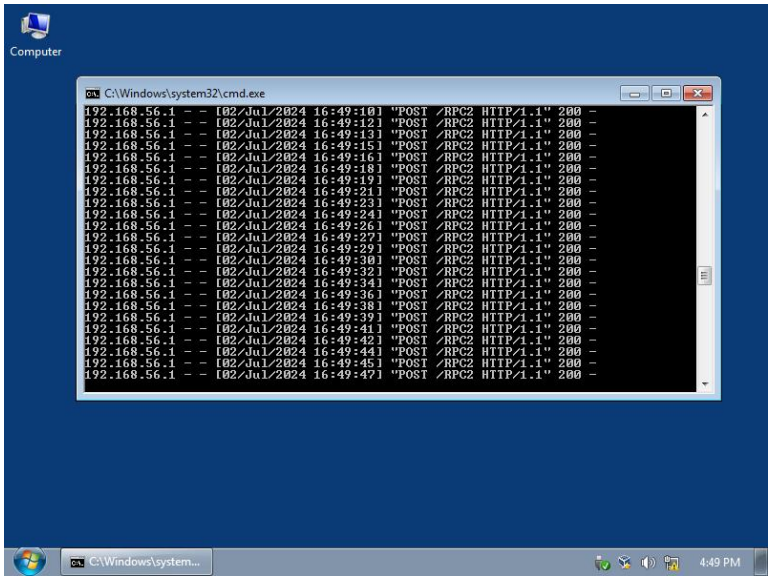

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process wi
th pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid
2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\
user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044
bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:48 PM

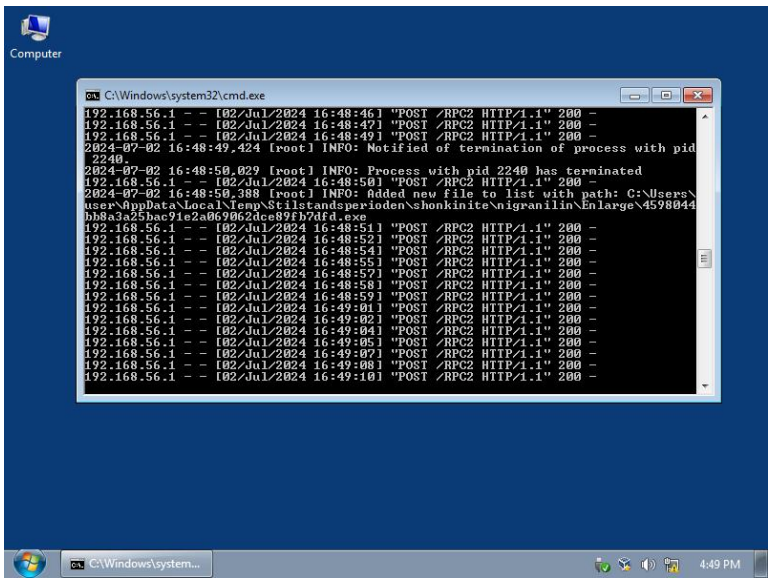

Computer
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
C:\Windows\system...
Regnfangs Setup: Ins...
C:\Windows\System...
4:48 PM

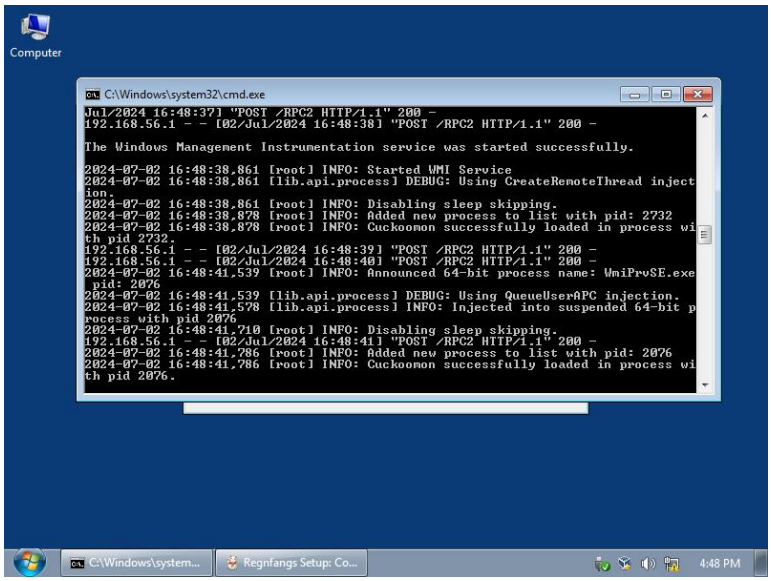

Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:34,392 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-07-02 16:48:34,410 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:34,427 [root] INFO: Added new process to list with pid: 556
2024-07-02 16:48:34,427 [root] INFO: Cuckoomon successfully loaded in process with pid 556.
192.168.56.1 - - [02/Jul/2024 16:48:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:35] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:36,609 [root] INFO: Starting WMI Service
The Windows Management Instrumentation service is starting.192.168.56.1 - - [02/Jul/2024 16:48:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:38] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-07-02 16:48:38,861 [root] INFO: Started WMI Service
2024-07-02 16:48:38,861 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-07-02 16:48:38,861 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:38,878 [root] INFO: Added new process to list with pid: 2732
2024-07-02 16:48:38,878 [root] INFO: Cuckoomon successfully loaded in process with pid 2732.
192.168.56.1 - - [02/Jul/2024 16:48:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:40] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

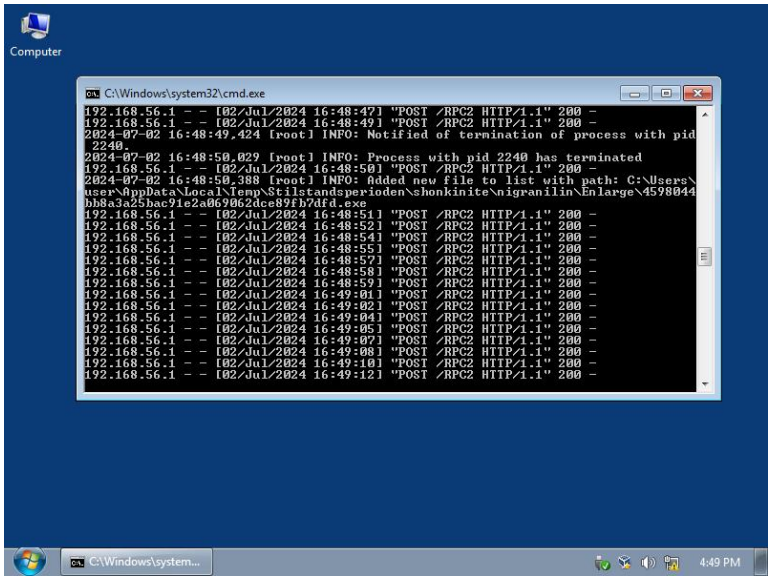

Computer
C:\Windows\system32\cmd.exe
The Windows Management Instrumentation service was started successfully.
2024-07-02 16:48:38,861 [root] INFO: Started WMI Service
2024-07-02 16:48:38,861 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-07-02 16:48:38,861 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:38,878 [root] INFO: Added new process to list with pid: 2732
2024-07-02 16:48:38,878 [root] INFO: Cuckoomon successfully loaded in process with pid 2732.
192.168.56.1 - - [02/Jul/2024 16:48:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:40] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,539 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2076
2024-07-02 16:48:41,539 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:41,578 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2076
2024-07-02 16:48:41,710 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [02/Jul/2024 16:48:41] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process with pid 2076.
192.168.56.1 - - [02/Jul/2024 16:48:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:45] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

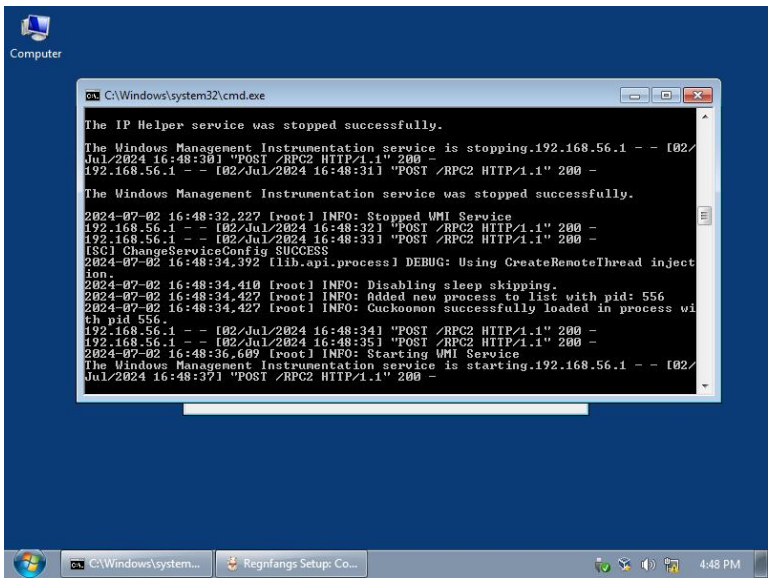

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:48] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:50] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:52] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

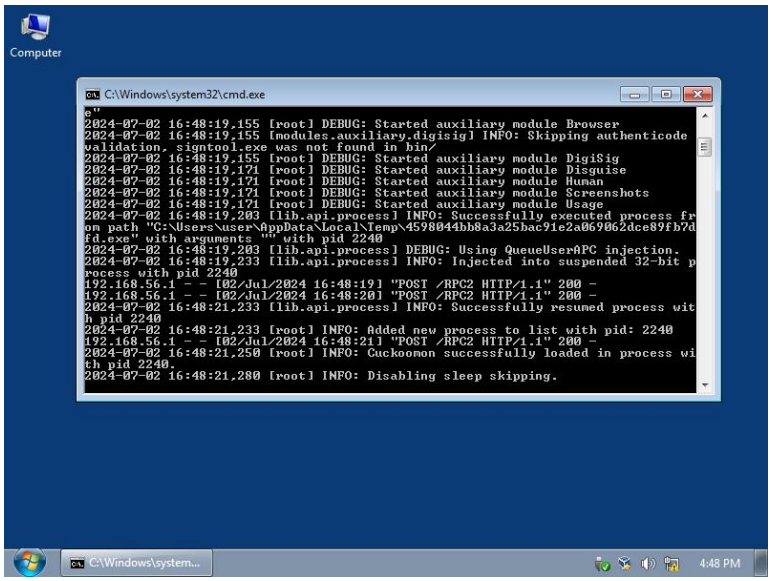

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:24] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:29] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:36] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:38] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:41] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:42] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:44] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:45] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:47] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

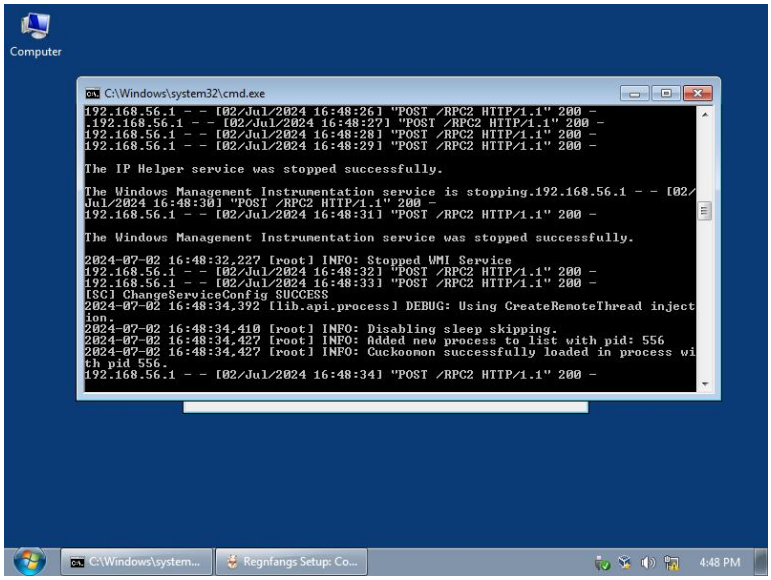

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:46] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid 2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM

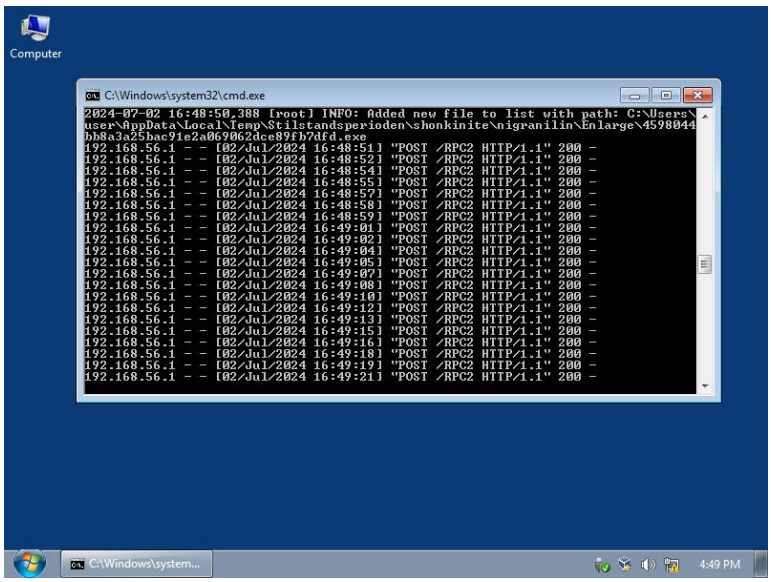

Computer
C:\Windows\system32\cmd.exe
Jul/2024 16:48:37] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:38] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was started successfully.
2024-07-02 16:48:38,861 [root] INFO: Started WMI Service
2024-07-02 16:48:38,861 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-07-02 16:48:38,861 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:38,878 [root] INFO: Added new process to list with pid: 2732
2024-07-02 16:48:38,878 [root] INFO: Cuckoomon successfully loaded in process with pid 2732.
192.168.56.1 - - [02/Jul/2024 16:48:39] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:40] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,539 [root] INFO: Announced 64-bit process name: WmiPrvSE.exe pid: 2076
2024-07-02 16:48:41,539 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:41,578 [lib.api.process] INFO: Injected into suspended 64-bit process with pid 2076
2024-07-02 16:48:41,710 [root] INFO: Disabling sleep skipping.
192.168.56.1 - - [02/Jul/2024 16:48:41] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:41,786 [root] INFO: Added new process to list with pid: 2076
2024-07-02 16:48:41,786 [root] INFO: Cuckoomon successfully loaded in process with pid 2076.
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM

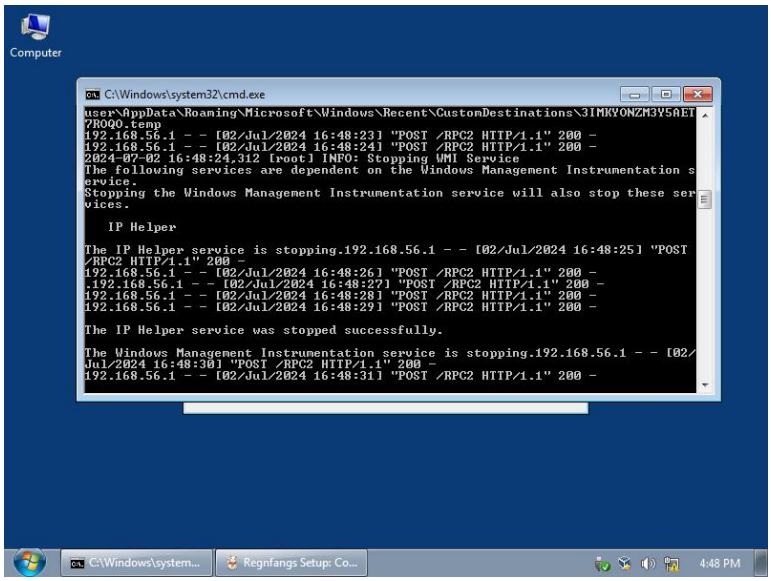

Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:47] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:49] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:49,424 [root] INFO: Notified of termination of process with pid 2240.
2024-07-02 16:48:50,029 [root] INFO: Process with pid 2240 has terminated
192.168.56.1 - - [02/Jul/2024 16:48:50] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM


Computer
C:\Windows\system32\cmd.exe
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:31] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was stopped successfully.
2024-07-02 16:48:32,227 [root] INFO: Stopped WMI Service
192.168.56.1 - - [02/Jul/2024 16:48:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:33] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-07-02 16:48:34,392 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-07-02 16:48:34,410 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:34,427 [root] INFO: Added new process to list with pid: 556
2024-07-02 16:48:34,427 [root] INFO: Cuckoomon successfully loaded in process with pid 556.
192.168.56.1 - - [02/Jul/2024 16:48:34] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:35] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:36,609 [root] INFO: Starting WMI Service
The Windows Management Instrumentation service is starting.192.168.56.1 - - [02/Jul/2024 16:48:37] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM


Computer
C:\Windows\system32\cmd.exe
e"
2024-07-02 16:48:19,155 [root] DEBUG: Started auxiliary module Browser
2024-07-02 16:48:19,155 [modules.auxiliary.digisig] INFO: Skipping authenticode validation, signtool.exe was not found in bin/
2024-07-02 16:48:19,155 [root] DEBUG: Started auxiliary module DigiSig
2024-07-02 16:48:19,171 [root] DEBUG: Started auxiliary module Disguise
2024-07-02 16:48:19,171 [root] DEBUG: Started auxiliary module Human
2024-07-02 16:48:19,171 [root] DEBUG: Started auxiliary module Screenshots
2024-07-02 16:48:19,171 [root] DEBUG: Started auxiliary module Usage
2024-07-02 16:48:19,203 [lib.api.process] INFO: Successfully executed process from path "C:\Users\user\AppData\Local\Temp\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe" with arguments "" with pid 2240
2024-07-02 16:48:19,203 [lib.api.process] DEBUG: Using QueueUserAPC injection.
2024-07-02 16:48:19,233 [lib.api.process] INFO: Injected into suspended 32-bit process with pid 2240
192.168.56.1 - - [02/Jul/2024 16:48:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:20] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:21,233 [lib.api.process] INFO: Successfully resumed process with pid 2240
2024-07-02 16:48:21,233 [root] INFO: Added new process to list with pid: 2240
192.168.56.1 - - [02/Jul/2024 16:48:21] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:21,250 [root] INFO: Cuckoomon successfully loaded in process with pid 2240.
2024-07-02 16:48:21,280 [root] INFO: Disabling sleep skipping.
C:\Windows\system...
4:48 PM


Computer
C:\Windows\system32\cmd.exe
192.168.56.1 - - [02/Jul/2024 16:48:26] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:29] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:31] "POST /RPC2 HTTP/1.1" 200 -
The Windows Management Instrumentation service was stopped successfully.
2024-07-02 16:48:32,227 [root] INFO: Stopped WMI Service
192.168.56.1 - - [02/Jul/2024 16:48:32] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:33] "POST /RPC2 HTTP/1.1" 200 -
[SC] ChangeServiceConfig SUCCESS
2024-07-02 16:48:34,392 [lib.api.process] DEBUG: Using CreateRemoteThread injection.
2024-07-02 16:48:34,410 [root] INFO: Disabling sleep skipping.
2024-07-02 16:48:34,427 [root] INFO: Added new process to list with pid: 556
2024-07-02 16:48:34,427 [root] INFO: Cuckoomon successfully loaded in process with pid 556.
192.168.56.1 - - [02/Jul/2024 16:48:34] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM


Computer
C:\Windows\system32\cmd.exe
2024-07-02 16:48:50,388 [root] INFO: Added new file to list with path: C:\Users\user\AppData\Local\Temp\Stilstandsperioden\shonkinite\nigranilin\Enlarge\4598044bb8a3a25bac91e2a069062dce89fb7dfd.exe
192.168.56.1 - - [02/Jul/2024 16:48:51] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:52] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:54] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:55] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:57] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:58] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:59] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:01] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:02] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:04] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:05] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:07] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:08] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:10] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:12] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:13] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:15] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:16] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:18] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:19] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:49:21] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
4:49 PM


Computer
C:\Windows\system32\cmd.exe
user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\3IMKYONZM3Y5AET
7RQQO.temp
192.168.56.1 - - [02/Jul/2024 16:48:23] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:24] "POST /RPC2 HTTP/1.1" 200 -
2024-07-02 16:48:24,312 [root] INFO: Stopping WMI Service
The following services are dependent on the Windows Management Instrumentation s
ervice.
Stopping the Windows Management Instrumentation service will also stop these ser
vices.
IP Helper
The IP Helper service is stopping.192.168.56.1 - - [02/Jul/2024 16:48:25] "POST
/RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:26] "POST /RPC2 HTTP/1.1" 200 -
.192.168.56.1 - - [02/Jul/2024 16:48:27] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:28] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:29] "POST /RPC2 HTTP/1.1" 200 -
The IP Helper service was stopped successfully.
The Windows Management Instrumentation service is stopping.192.168.56.1 - - [02/
Jul/2024 16:48:30] "POST /RPC2 HTTP/1.1" 200 -
192.168.56.1 - - [02/Jul/2024 16:48:31] "POST /RPC2 HTTP/1.1" 200 -
C:\Windows\system...
Regnfangs Setup: Co...
4:48 PM