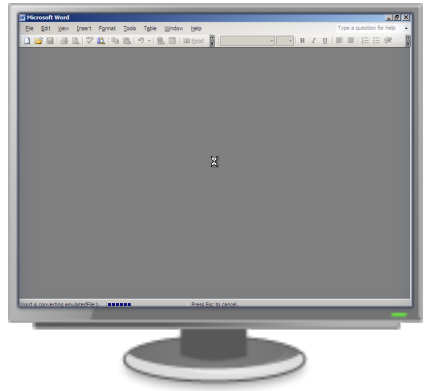
Emulated On: Microsoft Windows 7 32 bit, Office 2003 (11.5604.5606), Office 2007 (12.0.4518.1014), Adobe Acrobat Reader 9.0

1

BOA statement id 454-33-2463.doc

Malicious Activity Detected

Type	doc
MD5	84f7ff421517a558e2cdbb8c5294f7e5
SHA1	f46cc88a920f4e8a22d9abd2c8ec88a266d85a77



Emulation Screenshot

3 Affected Files

3 Files Created | 2 Files Modified | 1 File Deleted

C:\Users\admin\AppData\LocalLow\ofukd.ism
C:\Users\admin\AppData\Local\Temp\paw.exe
C:\Users\admin\AppData\Roaming\Uceso\uppu.exe

3 Affected Processes

3 Processes Created | 0 Processes Terminated | 0 Processes Crashed

C:\Program Files\Windows Mail\WinMail.exe
C:\Users\admin\AppData\Local\Temp\paw.exe
C:\Users\admin\AppData\Roaming\Uceso\uppu.exe

4 Affected Registry Keys

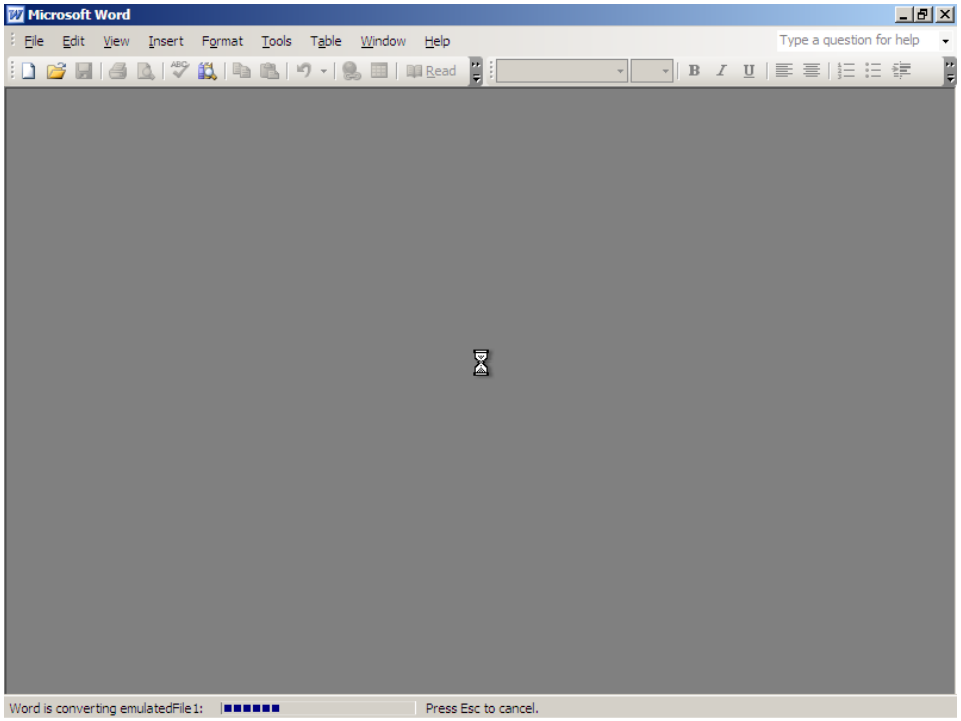
3 Entries Set | 1 Entry Deleted

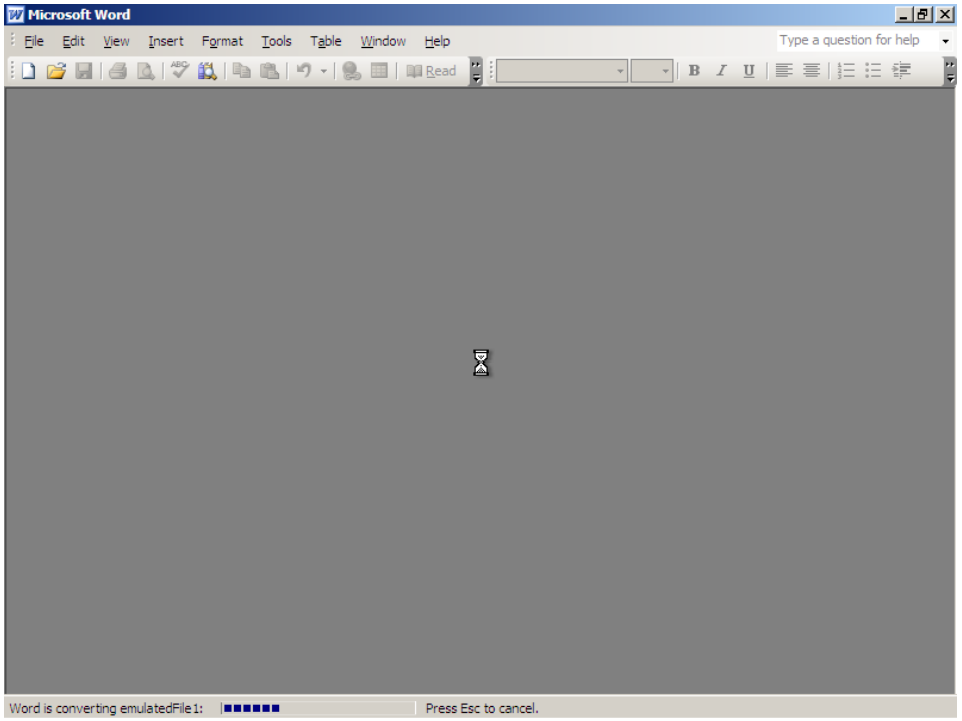
HKCU\Software\Microsoft\Keyvb\15fq6qj5
HKCU\Software\Microsoft\Keyvb\19bc8hhb
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\internat.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}

0 Attempted Network Connections

Malware Screen Shots

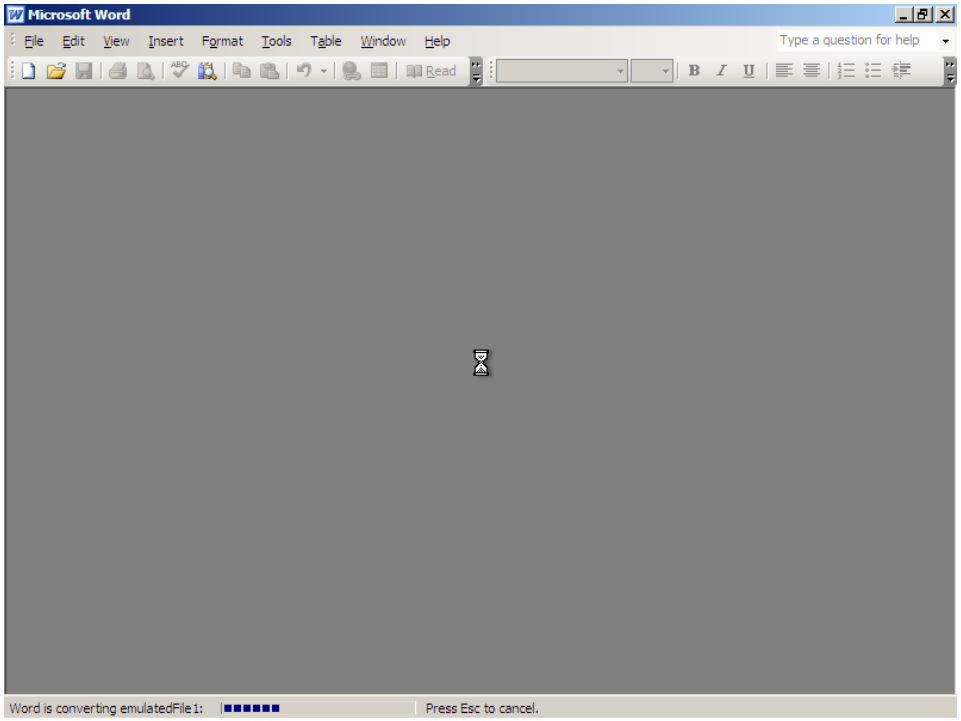
2





Malware Screen Shots

3



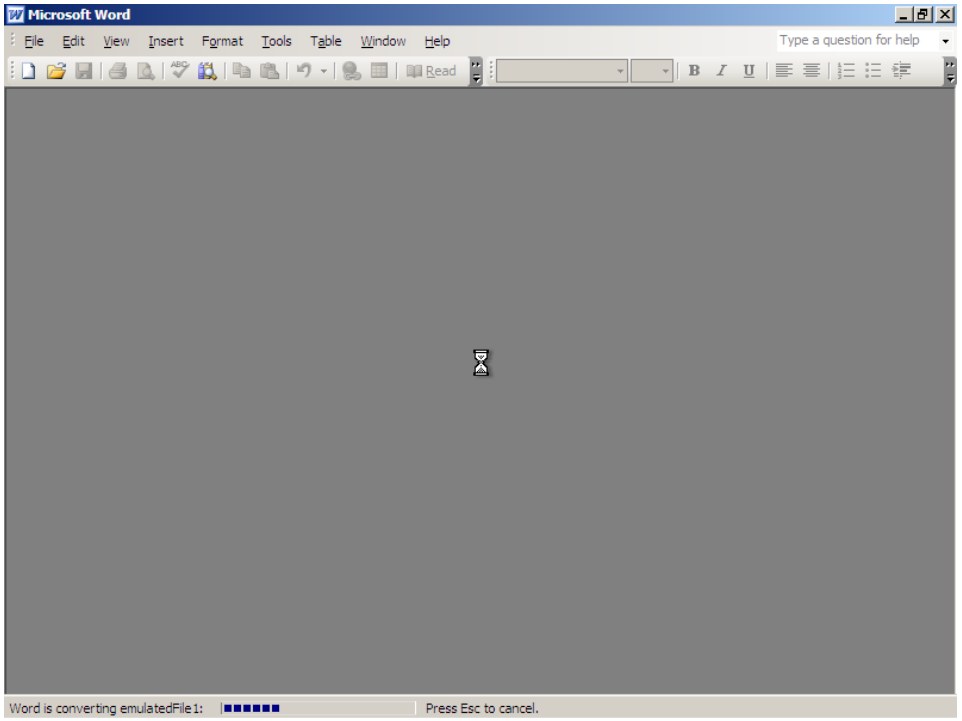


Table of Contents

Malware Residues

5

Processes Spawned or Interacted with
C:\Program Files\Windows Mail\WinMail.exe
C:\Users\admin\AppData\Local\Temp\paw.exe
C:\Users\admin\AppData\Roaming\Uceso\uppu.exe

Files Changed
C:\Users\admin\AppData\LocalLow\ofukd.ism
C:\Users\admin\AppData\Local\Temp\paw.exe
C:\Users\admin\AppData\Local\Temp\paw.exe
C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
C:\Users\admin\AppData\Roaming\Uceso\uppu.exe

Registry Keys Modified
HKCU\Software\Microsoft\Keyvb\15fg6gj5
HKCU\Software\Microsoft\Keyvb\19bc8hhb
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\internat.exe
HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}

Unexpected Activities By Time (1 out of 89)

6

Elapsed Time	Type	Action
00:00:19	Process creation	C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE **Created** C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:19	Process creation	C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE **Created** C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:19	File Create	C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE **Created** C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:19	File Write	C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE **Wrote To** C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:30	File Modify	C:\Users\admin\AppData\Local\Temp\paw.exe **Read From** C:\$Directory
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\winspool.drv
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\apphelp.dll
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\AppPatch\sysmain.sdb
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Local

Unexpected Activities By Time (2 out of 89)

7

Elapsed Time	Type	Action
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Local\Temp
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\imm32.dll
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Terminal Server\TSAppCompat
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Terminal Server\TSUserEnabled
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\Terminal Server
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\ShowDebugInfo
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Session Manager\SafeDllSearchMode

Unexpected Activities By Time (3 out of 89)

8

Elapsed Time	Type	Action
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32\paw
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU
00:00:30	Registry Enumerate	C:\Users\admin\AppData\Local\Temp\paw.exe **Enumerate** HKCU\Control Panel\Desktop\LanguageConfiguration
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU\Control Panel\Desktop\LanguageConfiguration
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKCU\Control Panel\Desktop\PreferredUILanguages
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU\Control Panel\Desktop
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKCU\Control Panel\Desktop\MuiCached\MachinePreferredUILanguages
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU\Control Panel\Desktop\MuiCached
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs

Unexpected Activities By Time (4 out of 89)

9

Elapsed Time	Type	Action
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\sechost.dll
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\secur32.dll
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\sspicli.dll
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\netapi32.dll
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\netutils.dll
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\srvcli.dll
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\wkscli.dll
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\samcli.dll
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\IPHLPAPI.DLL
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\winnsi.dll
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\version.dll
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\Globalization\Sorting\SortDefault.nls
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Roaming

Unexpected Activities By Time (5 out of 89)

10

Elapsed Time	Type	Action
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\profapi.dll
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\LocalLow
00:00:30	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:30	File Modify	C:\Users\admin\AppData\Local\Temp\paw.exe **Read From** C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorUseSystemHeap
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Ole
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorSystemHeapIsPrivate
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Ole
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\crypt32
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters\RpcCacheTimeout

Unexpected Activities By Time (6 out of 89)

11

Elapsed Time	Type	Action
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\SQMClient\Windows
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\WinSock_Registry_Version
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale
00:00:30	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\AppId_Catalog
00:00:30	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Callout
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Serial_Access_Num
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Next_Catalog_Entry_ID
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Num_Catalog_Entries
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001

Unexpected Activities By Time (7 out of 89)

12

Elapsed Time	Type	Action
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009\PackedCatalogItem

Unexpected Activities By Time (8 out of 89)

13

Elapsed Time	Type	Action
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000014\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000014
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000015\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000015
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000016\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000016

Unexpected Activities By Time (9 out of 89)

14

Elapsed Time	Type	Action
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000017\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000017
00:00:31	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018\PackedCatalogItem
00:00:31	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018
00:00:32	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000019\PackedCatalogItem
00:00:32	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000019
00:00:32	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000020\PackedCatalogItem
00:00:32	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000020
00:00:32	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000021\PackedCatalogItem
00:00:32	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000021
00:00:32	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000022\PackedCatalogItem
00:00:32	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000022
00:00:32	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000023\PackedCatalogItem
00:00:32	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000023
00:00:32	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000024\PackedCatalogItem

Unexpected Activities By Time (10 out of 89)

15

Elapsed Time	Type	Action
00:00:32	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000024
00:00:32	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries
00:00:32	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Serial_Access_Num
00:00:32	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Num_Catalog_Entries
00:00:32	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\LibraryPath
00:00:32	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\DisplayString
00:00:32	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\ProviderId
00:00:32	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\AddressFamily
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\SupportedNameSpace
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\Enabled
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\Version
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\StoresServiceClassInfo
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\ProviderInfo
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\LibraryPath

Unexpected Activities By Time (11 out of 89)

16

Elapsed Time	Type	Action
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\DisplayString
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\ProviderId
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\AddressFamily
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\SupportedNameSpace
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\Enabled
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\Version
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\StoresServiceClassInfo
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\ProviderInfo
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\LibraryPath
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\DisplayString
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\ProviderId
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\AddressFamily
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\SupportedNameSpace
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\Enabled

Unexpected Activities By Time (12 out of 89)

17

Elapsed Time	Type	Action
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\Version
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\StoresServiceClassInfo
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\ProviderInfo
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\LibraryPath
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\DisplayString
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\ProviderId
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\AddressFamily
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\SupportedNameSpace
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\Enabled
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\Version
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\StoresServiceClassInfo
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\ProviderInfo
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\LibraryPath

Unexpected Activities By Time (13 out of 89)

18

Elapsed Time	Type	Action
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\DisplayString
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\ProviderId
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\AddressFamily
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\SupportedNameSpace
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\Enabled
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\Version
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\StoresServiceClassInfo
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\ProviderInfo
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\LibraryPath
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\DisplayString
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\ProviderId
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\AddressFamily
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\SupportedNameSpace
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\Enabled

Unexpected Activities By Time (14 out of 89)

19

Elapsed Time	Type	Action
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\Version
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\StoresServiceClassInfo
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\ProviderInfo
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Ws2_32NumHandleBuckets
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Rpc\MaxRpcSize
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Rpc
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName\ComputerName
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\Setup\OOBEInProgress
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\Setup
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\Setup\SystemSetupInProgress

Unexpected Activities By Time (15 out of 89)

20

Elapsed Time	Type	Action
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\Setup
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\SQMClient\Windows
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Category
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Name
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\ParentFolder
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Description
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\RelativePath
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\ParsingName
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\InfoTip
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\LocalizedName
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Icon
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Security
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\StreamResource

Unexpected Activities By Time (16 out of 89)

21

Elapsed Time	Type	Action
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\StreamResourceType
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\LocalRedirectOnly
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Roamable
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PreCreate
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Stream
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PublishExpandedPath
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Attributes
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\FolderTypeID
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\InitFolderHandler
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Category
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Name
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\ParentFolder
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Description

Unexpected Activities By Time (17 out of 89)

22

Elapsed Time	Type	Action
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\RelativePath
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\ParsingName
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\InfoTip
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\LocalizedName
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Icon
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Security
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\StreamResource
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\StreamResourceType
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\LocalRedirectOnly
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Roamable
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\PreCreate
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Stream
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\PublishExpandedPath
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Attributes
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\FolderTypeID

Unexpected Activities By Time (18 out of 89)

23

Elapsed Time	Type	Action
00:00:37	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\InitFolderHandler
00:00:37	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}
00:00:38	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
00:00:38	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
00:00:38	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
00:00:38	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Category
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Name
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\ParentFolder
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Description
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\RelativePath
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\ParsingName
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\InfoTip
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\LocalizedName

Unexpected Activities By Time (19 out of 89)

Elapsed Time	Type	Action
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Icon
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Security
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\StreamResource
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\StreamResourceType
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\LocalRedirectOnly
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Roamable
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\PreCreate
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Stream
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\PublishExpandedPath
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Attributes
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\FolderTypeID
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\InitFolderHandler
00:00:38	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}
00:00:38	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
00:00:38	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU

Unexpected Activities By Time (20 out of 89)

Elapsed Time	Type	Action
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\{A520A1A4-1780-4FF6-BD18-167343C5AF16}
00:00:38	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Category
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Name
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParentFolder
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Description
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\RelativePath
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParsingName
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InfoTip
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalizedName
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Icon
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Security
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResource
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResourceType
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalRedirectOnly

Unexpected Activities By Time (21 out of 89)

Elapsed Time	Type	Action
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Roamable
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PreCreate
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Stream
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PublishExpandedPath
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Attributes
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\FolderTypeID
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InitFolderHandler
00:00:38	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}
00:00:38	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-292738990-2461527479-3432112557-1000\ProfileImagePath
00:00:38	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-292738990-2461527479-3432112557-1000
00:00:38	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
00:00:39	File Modify	C:\Users\admin\AppData\Local\Temp\paw.exe **Read From** C:\$Mft
00:00:39	File Create	C:\Users\admin\AppData\Local\Temp\paw.exe **Created** C:\Users\admin\AppData\Roaming\Uceso
00:00:39	File Modify	C:\Users\admin\AppData\Local\Temp\paw.exe **Read From** C:\$Mft
00:00:39	File Create	C:\Users\admin\AppData\Local\Temp\paw.exe **Created** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe

Unexpected Activities By Time (22 out of 89)

27

Elapsed Time	Type	Action
00:00:39	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\cryptsp.dll
00:00:39	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\rsaenh.dll
00:00:39	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\cryptbase.dll
00:00:39	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows
00:00:39	File Modify	C:\Users\admin\AppData\Local\Temp\paw.exe **Read From** C:\$Directory
00:00:39	File Modify	C:\Users\admin\AppData\Local\Temp\paw.exe **Read From** C:\$Mft
00:00:39	File Create	C:\Users\admin\AppData\Local\Temp\paw.exe **Created** C:\Users\admin\AppData\LocalLow\ofukd.ism
00:00:39	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\LocalLow
00:00:39	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:39	File Modify	C:\Users\admin\AppData\Local\Temp\paw.exe **Read From** C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:39	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	File Delete	C:\Users\admin\AppData\Local\Temp\paw.exe **Deleted** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	File Create	C:\Users\admin\AppData\Local\Temp\paw.exe **Created** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	File Write	C:\Users\admin\AppData\Local\Temp\paw.exe **Wrote To** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Roaming

Unexpected Activities By Time (23 out of 89)

28

Elapsed Time	Type	Action
00:00:39	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Roaming\Uceso
00:00:39	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Roaming
00:00:39	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	Process creation	C:\Users\admin\AppData\Local\Temp\paw.exe **Created** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU\Software\Microsoft\Keyvb
00:00:39	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU\Software\Microsoft
00:00:39	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName\ComputerName
00:00:39	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName
00:00:39	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\Setup\OOBEInProgress
00:00:39	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\Setup
00:00:39	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\Setup\SystemSetupInProgress
00:00:39	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\Setup
00:00:39	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\ComputerName
00:00:39	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate

Unexpected Activities By Time (24 out of 89)

Elapsed Time	Type	Action
00:00:39	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DigitalProductId
00:00:40	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced Cryptographic Provider v1.0\Type
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced Cryptographic Provider v1.0\Image Path
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Session Manager\SafeProcessSearchMode
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy\Enabled
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy
00:00:40	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy
00:00:40	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\Lsa
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Policies\Microsoft\Cryptography\PrivKeyCacheMaxItems
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Policies\Microsoft\Cryptography\PrivKeyCachePurgeIntervalSeconds
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Policies\Microsoft\Cryptography\PrivateKeyLifetimeSeconds
00:00:40	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Policies\Microsoft\Cryptography
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid
00:00:40	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Cryptography

Unexpected Activities By Time (25 out of 89)

Elapsed Time	Type	Action
00:00:40	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced Cryptographic Provider v1.0
00:00:40	File Write	C:\Users\admin\AppData\Local\Temp\paw.exe **Wrote To** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\AuthenticodeEnabled
00:00:40	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
00:00:40	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DisableLocalOverride
00:00:40	Registry Query	C:\Users\admin\AppData\Local\Temp\paw.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
00:00:40	Registry Close	C:\Users\admin\AppData\Local\Temp\paw.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide
00:00:40	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\System32\apphelp.dll
00:00:40	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\AppPatch\sysmain.sdb
00:00:40	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Roaming\Uceso

Unexpected Activities By Time (26 out of 89)

31

Elapsed Time	Type	Action
00:00:40	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\
00:00:40	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users
00:00:40	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin
00:00:40	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData
00:00:40	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Roaming
00:00:40	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Roaming\Uceso
00:00:40	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	File Modify	C:\Users\admin\AppData\Local\Temp\paw.exe **Read From** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	File Open	C:\Users\admin\AppData\Local\Temp\paw.exe **Opened** C:\Windows\AppPatch\sysmain.sdb
00:00:40	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Terminal Server\TSAppCompat
00:00:40	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Terminal Server\TSUserEnabled
00:00:40	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\Terminal Server
00:00:40	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled
00:00:40	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers

Unexpected Activities By Time (27 out of 89)

32

Elapsed Time	Type	Action
00:00:40	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\ShowDebugInfo
00:00:40	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags
00:00:40	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
00:00:40	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
00:00:40	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
00:00:40	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
00:00:40	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Session Manager\SafeDllSearchMode
00:00:40	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
00:00:40	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
00:00:40	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32\uppu
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU
00:00:41	Registry Enumerate	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Enumerate** HKCU\Control Panel\Desktop\LanguageConfiguration
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU\Control Panel\Desktop\LanguageConfiguration

Unexpected Activities By Time (28 out of 89)

33

Elapsed Time	Type	Action
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU
00:00:41	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKCU\Control Panel\Desktop\PreferredUILanguages
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU\Control Panel\Desktop
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU
00:00:41	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKCU\Control Panel\Desktop\MuiCached\MachinePreferredUILanguages
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU\Control Panel\Desktop\MuiCached
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU
00:00:41	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
00:00:41	File Modify	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Read From** C:\$Directory
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Users\admin\AppData\Roaming
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\winspool.drv
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\apphelp.dll
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\AppPatch\sysmain.sdb
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe

Unexpected Activities By Time (29 out of 89)

34

Elapsed Time	Type	Action
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Users
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Users\admin
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Users\admin\AppData
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Users\admin\AppData\Roaming
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Users\admin\AppData\Roaming\Uceso
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\imm32.dll
00:00:41	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorUseSystemHeap
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Ole
00:00:41	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorSystemHeapIsPrivate
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Ole
00:00:41	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\crypt32
00:00:41	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

Unexpected Activities By Time (30 out of 89)

35

Elapsed Time	Type	Action
00:00:41	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
00:00:41	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\sechost.dll
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\secur32.dll
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\sspicli.dll
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\netapi32.dll
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\netutils.dll
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\srvcli.dll
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\wkscli.dll
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\samcli.dll
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\IPHLPAPI.DLL
00:00:41	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\winnsi.dll
00:00:42	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\version.dll
00:00:42	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\Globalization\Sorting\SortDefault.nls
00:00:42	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows

Unexpected Activities By Time (31 out of 89)

Elapsed Time	Type	Action
00:00:42	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Users\admin\AppData\Roaming
00:00:42	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Windows\System32\profapi.dll
00:00:42	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Users\admin\AppData\LocalLow
00:00:42	File Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Opened** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:42	File Modify	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Read From** C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters\RpcCacheTimeout
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\SQMClient\Windows
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\WinSock_Registry_Version
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\AppId_Catalog

Unexpected Activities By Time (32 out of 89)

37

Elapsed Time	Type	Action
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Callout
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Serial_Access_Num
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Next_Catalog_Entry_ID
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Num_Catalog_Entries
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001\PackedCatalogItem
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002\PackedCatalogItem
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003\PackedCatalogItem
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004\PackedCatalogItem
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005\PackedCatalogItem
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006\PackedCatalogItem

Unexpected Activities By Time (33 out of 89)

38

Elapsed Time	Type	Action
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007\PackedCatalogItem
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008\PackedCatalogItem
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009\PackedCatalogItem
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010\PackedCatalogItem
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010
00:00:42	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011\PackedCatalogItem
00:00:42	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012\PackedCatalogItem
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013\PackedCatalogItem
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013

Unexpected Activities By Time (34 out of 89)

39

Elapsed Time	Type	Action
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000014\PackedCatalogItem
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000014
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000015\PackedCatalogItem
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000015
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000016\PackedCatalogItem
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000016
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000017\PackedCatalogItem
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000017
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018\PackedCatalogItem
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000019\PackedCatalogItem
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000019
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000020\PackedCatalogItem
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000020
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000021\PackedCatalogItem

Unexpected Activities By Time (35 out of 89)

40

Elapsed Time	Type	Action
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000021
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000022\PackedCatalogItem
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000022
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000023\PackedCatalogItem
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000023
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000024\PackedCatalogItem
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000024
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Serial_Access_Num
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Num_Catalog_Entries
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\LibraryPath
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\DisplayString
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\ProviderId
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\AddressFamily
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\SupportedNameSpace

Unexpected Activities By Time (36 out of 89)

41

Elapsed Time	Type	Action
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\Enabled
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\Version
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\StoresServiceClassInfo
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\ProviderInfo
00:00:43	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\LibraryPath
00:00:43	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\DisplayString
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\ProviderId
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\AddressFamily
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\SupportedNameSpace
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\Enabled
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\Version
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\StoresServiceClassInfo
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\ProviderInfo
00:00:44	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002

Unexpected Activities By Time (37 out of 89)

Elapsed Time	Type	Action
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\LibraryPath
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\DisplayString
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\ProviderId
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\AddressFamily
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\SupportedNameSpace
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\Enabled
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\Version
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\StoresServiceClassInfo
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\ProviderInfo
00:00:44	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\LibraryPath
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\DisplayString
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\ProviderId
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\AddressFamily
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\SupportedNameSpace

Unexpected Activities By Time (38 out of 89)

Elapsed Time	Type	Action
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\Enabled
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\Version
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\StoresServiceClassInfo
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\ProviderInfo
00:00:44	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\LibraryPath
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\DisplayString
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\ProviderId
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\AddressFamily
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\SupportedNameSpace
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\Enabled
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\Version
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\StoresServiceClassInfo
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\ProviderInfo
00:00:44	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005

Unexpected Activities By Time (39 out of 89)

Elapsed Time	Type	Action
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\LibraryPath
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\DisplayString
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\ProviderId
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\AddressFamily
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\SupportedNameSpace
00:00:44	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\Enabled
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\Version
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\StoresServiceClassInfo
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\ProviderInfo
00:00:45	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006
00:00:45	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries
00:00:45	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Ws2_32NumHandleBuckets
00:00:45	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Rpc\MaxRpcSize

Unexpected Activities By Time (40 out of 89)

Elapsed Time	Type	Action
00:00:45	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Rpc
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName\ComputerName
00:00:45	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\Setup\OOBEInProgress
00:00:45	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\Setup
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SYSTEM\Setup\SystemSetupInProgress
00:00:45	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SYSTEM\Setup
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
00:00:45	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\SQMClient\Windows
00:00:45	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Category
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Name
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\ParentFolder
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Description
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\RelativePath

Unexpected Activities By Time (41 out of 89)

Elapsed Time	Type	Action
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\ParsingName
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\InfoTip
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\LocalizedName
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Icon
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Security
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\StreamResource
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\StreamResourceType
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\LocalRedirectOnly
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Roamable
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PreCreate
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Stream
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PublishExpandedPath
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Attributes
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\FolderTypeID
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\InitFolderHandler

Unexpected Activities By Time (42 out of 89)

Elapsed Time	Type	Action
00:00:45	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}
00:00:45	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Category
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Name
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\ParentFolder
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Description
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\RelativePath
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\ParsingName
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\InfoTip
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\LocalizedName
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Icon
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Security
00:00:45	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\StreamResource
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\StreamResourceType
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\LocalRedirectOnly

Unexpected Activities By Time (43 out of 89)

Elapsed Time	Type	Action
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Roamable
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\PreCreate
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Stream
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\PublishExpandedPath
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Attributes
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\FolderTypeID
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\InitFolderHandler
00:00:46	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}
00:00:46	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
00:00:46	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
00:00:46	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
00:00:46	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Category
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Name

Unexpected Activities By Time (44 out of 89)

Elapsed Time	Type	Action
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\ParentFolder
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Description
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\RelativePath
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\ParsingName
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\InfoTip
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\LocalizedName
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Icon
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Security
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\StreamResource
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\StreamResourceType
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\LocalRedirectOnly
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Roamable
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\PreCreate
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Stream
00:00:46	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\PublishExpandedPath

Unexpected Activities By Time (45 out of 89)

Elapsed Time	Type	Action
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Attributes
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\FolderTypeID
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\InitFolderHandler
00:00:47	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}
00:00:47	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
00:00:47	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\{A520A1A4-1780-4FF6-BD18-167343C5AF16}
00:00:47	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Category
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Name
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParentFolder
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Description
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\RelativePath
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParsingName
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InfoTip

Unexpected Activities By Time (46 out of 89)

Elapsed Time	Type	Action
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalizedName
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Icon
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Security
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResource
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResourceType
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalRedirectOnly
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Roamable
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PreCreate
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Stream
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PublishExpandedPath
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Attributes
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\FolderTypeID
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InitFolderHandler
00:00:47	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-292738990-2461527479-3432112557-1000\ProfileImagePath

Unexpected Activities By Time (47 out of 89)

Elapsed Time	Type	Action
00:00:47	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-292738990-2461527479-3432112557-1000
00:00:47	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKCU\Software\Microsoft\Keyvb\19bc8hhb
00:00:47	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU\Software\Microsoft\Keyvb
00:00:47	Registry Query	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Queried** HKCU\Software\Microsoft\Keyvb\15fg6gj5
00:00:47	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU\Software\Microsoft\Keyvb
00:00:47	Registry Set	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Set** HKCU\Software\Microsoft\Keyvb\15fg6gj5
00:00:47	Registry Close	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe **Closed** HKCU\Software\Microsoft\Keyvb
00:00:52	Registry Set	C:\Windows\System32\taskhost.exe **Set** HKCU\Software\Microsoft\Keyvb\19bc8hhb
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters\RpcCacheTimeout
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters

Unexpected Activities By Time (48 out of 89)

Elapsed Time	Type	Action
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\WinSock_Registry_Version
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\AppId_Catalog
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Callout
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Serial_Access_Num
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Next_Catalog_Entry_ID
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Num_Catalog_Entries
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005\PackedCatalogItem

Unexpected Activities By Time (49 out of 89)

Elapsed Time	Type	Action
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012

Unexpected Activities By Time (50 out of 89)

Elapsed Time	Type	Action
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000014\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000014
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000015\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000015
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000016\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000016
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000017\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000017
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000019\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000019
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000020\PackedCatalogItem

Unexpected Activities By Time (51 out of 89)

Elapsed Time	Type	Action
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000020
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000021\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000021
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000022\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000022
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000023\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000023
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000024\PackedCatalogItem
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000024
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Serial_Access_Num
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Num_Catalog_Entries
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\LibraryPath
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\DisplayString
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\ProviderId

Unexpected Activities By Time (52 out of 89)

Elapsed Time	Type	Action
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\AddressFamily
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\SupportedNameSpace
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\Enabled
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\Version
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\StoresServiceClassInfo
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\ProviderInfo
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\LibraryPath
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\DisplayString
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\ProviderId
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\AddressFamily
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\SupportedNameSpace
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\Enabled
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\Version
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\StoresServiceClassInfo

Unexpected Activities By Time (53 out of 89)

Elapsed Time	Type	Action
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\ProviderInfo
00:00:52	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\LibraryPath
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\DisplayString
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\ProviderId
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\AddressFamily
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\SupportedNameSpace
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\Enabled
00:00:52	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\Version
00:00:53	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\StoresServiceClassInfo
00:00:53	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\ProviderInfo
00:00:53	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003
00:00:53	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\LibraryPath
00:00:53	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\DisplayString
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\ProviderId

Unexpected Activities By Time (54 out of 89)

Elapsed Time	Type	Action
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\AddressFamily
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\SupportedNameSpace
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\Enabled
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\Version
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\StoresServiceClassInfo
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\ProviderInfo
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\LibraryPath
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\DisplayString
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\ProviderId
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\AddressFamily
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\SupportedNameSpace
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\Enabled
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\Version
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32\secur32.dll

Unexpected Activities By Time (55 out of 89)

Elapsed Time	Type	Action
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32\sspicli.dll
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32\netapi32.dll
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32\netutils.dll
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32\srvcli.dll
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32\wkscli.dll
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32\samcli.dll
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32\IPHLPAPI.DLL
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32\winnsi.dll
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32\dwm.exe
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32\userenv.dll
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Windows\System32\profapi.dll
00:00:58	File Modify	C:\Windows\System32\dwm.exe **Read From** C:\$Mft
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Users\admin\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates
00:00:58	File Modify	C:\Windows\System32\dwm.exe **Read From** C:\$Mft

Unexpected Activities By Time (56 out of 89)

Elapsed Time	Type	Action
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Users\admin\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs
00:00:58	File Modify	C:\Windows\System32\dwm.exe **Read From** C:\$Mft
00:00:58	File Open	C:\Windows\System32\dwm.exe **Opened** C:\Users\admin\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\StoresServiceClassInfo
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\ProviderInfo
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\LibraryPath
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\DisplayString
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\ProviderId
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\AddressFamily
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\SupportedNameSpace
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\Enabled
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\Version
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\StoresServiceClassInfo
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\ProviderInfo

Unexpected Activities By Time (57 out of 89)

Elapsed Time	Type	Action
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Ws2_32NumHandleBuckets
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Category
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Name
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\ParentFolder
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Description
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\RelativePath
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\ParsingName
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\InfoTip
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\LocalizedName
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Icon

Unexpected Activities By Time (58 out of 89)

Elapsed Time	Type	Action
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Security
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\StreamResource
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\StreamResourceType
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\LocalRedirectOnly
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Roamable
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\PreCreate
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Stream
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\PublishExpandedPath
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Attributes
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\FolderTypeID
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\InitFolderHandler
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKCU\Software\Microsoft\Keyvb\19bc8hhb
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKCU\Software\Microsoft\Keyvb
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\crypt32\DiagLevel

Unexpected Activities By Time (59 out of 89)

Elapsed Time	Type	Action
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\crypt32\DiagMatchAnyMask
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\crypt32
00:00:58	Registry Enumerate	C:\Windows\System32\dwm.exe **Enumerated** HKLM\SOFTWARE\Microsoft\Cryptography\OID
00:00:58	Registry Enumerate	C:\Windows\System32\dwm.exe **Enumerated** HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Read** HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\#16
00:00:58	Registry Enumerate	C:\Windows\System32\dwm.exe **Enumerate** HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\#16
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\#16
00:00:58	Registry Enumerate	C:\Windows\System32\dwm.exe **Enumerated** HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Read** HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\Ldap
00:00:58	Registry Enumerate	C:\Windows\System32\dwm.exe **Enumerate** HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\Ldap
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\Ldap
00:00:58	Registry Enumerate	C:\Windows\System32\dwm.exe **Enumerated** HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0
00:00:58	Registry Enumerate	C:\Windows\System32\dwm.exe **Enumerated** HKLM\SOFTWARE\Microsoft\Cryptography\OID

Unexpected Activities By Time (60 out of 89)

Elapsed Time	Type	Action
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 1
00:00:58	Registry Enumerate	C:\Windows\System32\dwm.exe **Enumerated** HKLM\SOFTWARE\Microsoft\Cryptography\OID
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SOFTWARE\Microsoft\Cryptography\OID
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKCU
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKCU\Software\Microsoft\SystemCertificates\My
00:00:58	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-292738990-2461527479-3432112557-1000\ProfileImagePath
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-292738990-2461527479-3432112557-1000
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKCU
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKCU\Software\Microsoft\SystemCertificates\My
00:00:58	Registry Set	C:\Windows\System32\dwm.exe **Set** HKCU\Software\Microsoft\Keyvb\19bc8hhb
00:00:58	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKCU\Software\Microsoft\Keyvb
00:00:59	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\crypt32\DiagLevel
00:00:59	Registry Query	C:\Windows\System32\dwm.exe **Queried** HKLM\SYSTEM\ControlSet001\services\crypt32\DiagMatchAnyMask
00:00:59	Registry Close	C:\Windows\System32\dwm.exe **Closed** HKLM\SYSTEM\ControlSet001\services\crypt32
00:00:59	Registry Set	C:\Windows\System32\taskhost.exe **Set** HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}

Unexpected Activities By Time (61 out of 89)

Elapsed Time	Type	Action
00:00:59	Registry Deleted	C:\Windows\System32\taskhost.exe **Deleted** HKCU\Software\Microsoft\Windows\CurrentVersion\Run\internat.exe
00:00:59	Registry Set	C:\Windows\System32\taskhost.exe **Set** HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}
00:00:59	Process creation	C:\Windows\System32\svchost.exe **Created** C:\Program Files\Windows Mail\WinMail.exe
00:00:59	Registry Set	C:\Windows\System32\taskhost.exe **Set** HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}
00:00:59	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\$Mft
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Prefetch\WINMAIL.EXE-1092D371.pf
00:00:59	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Prefetch\WINMAIL.EXE-1092D371.pf
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:
00:00:59	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\$Mft
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\$EXTEND
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files\Common Files
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files\Common Files\System
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files\Windows Mail
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files\Windows Mail\en-US

Unexpected Activities By Time (62 out of 89)

Elapsed Time	Type	Action
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\ProgramData
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\ProgramData\Microsoft
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\ProgramData\Microsoft\User Account Pictures
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Users
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Users\admin
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Users\admin\AppData
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Users\admin\AppData\Local
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Users\admin\AppData\Local\Microsoft
00:00:59	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\$Mft
00:00:59	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Users\admin\AppData\Local\Microsoft\Windows Mail
00:01:00	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Users\admin\AppData\Local\Microsoft\Windows Mail
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Users\admin\AppData\Local\Temp
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Fonts
00:01:00	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Fonts

Unexpected Activities By Time (63 out of 89)

Elapsed Time	Type	Action
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Globalization
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Globalization\Sorting
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\inf
00:01:00	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\inf
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32
00:01:00	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\drivers
00:01:00	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\drivers
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\en-US
00:01:00	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\en-US
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7600.16385_none_72fc7cbf861225ca
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\ntdll.dll
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files\Windows Mail\WinMail.exe
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\kernel32.dll

Unexpected Activities By Time (64 out of 89)

Elapsed Time	Type	Action
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\apisetschema.dll
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\KernelBase.dll
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\locale.nls
00:01:00	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\advapi32.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msvcrt.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\sechost.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\rpcrt4.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\user32.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\gdi32.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\lpk.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\usp10.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msoert2.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\ole32.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\oleaut32.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\shlwapi.dll

Unexpected Activities By Time (65 out of 89)

Elapsed Time	Type	Action
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\shell32.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\imm32.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msctf.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files\Windows Mail\en-US\WinMail.exe.mui
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\WindowsShell.Manifest
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Globalization\Sorting\SortDefault.nls
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\rpcss.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\cryptbase.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\uxtheme.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Fonts\plantc.ttf
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\cryptdlg.dll
00:01:01	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\wintrust.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\crypt32.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msasn1.dll

Unexpected Activities By Time (66 out of 89)

Elapsed Time	Type	Action
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\cryptui.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\imagehlp.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msimg32.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\secur32.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\sspicli.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\wininet.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\normaliz.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\urlmon.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\iertutil.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msftedit.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Fonts\phagspab.ttf
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Fonts\simfang.ttf
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\profapi.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\propsys.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\clbcatq.dll

Unexpected Activities By Time (67 out of 89)

Elapsed Time	Type	Action
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Fonts\phagspa.ttf
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\cryptsp.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\rsaenh.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\RpcRtRemote.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files\Common Files\System\wab32.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msxml6.dll
00:01:02	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\en-US\KernelBase.dll.mui
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msxml6r.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Fonts\nyala.ttf
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7600.16385_none_72fc7cbf861225ca\GdiPlus.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files\Common Files\System\wab32res.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\shacct.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\samlib.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\ProgramData\Microsoft\User Account Pictures\user.bmp
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Users\admin\AppData\Local\Temp\admin.bmp

Unexpected Activities By Time (68 out of 89)

Elapsed Time	Type	Action
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Fonts\ntailu.ttf
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\atl.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msoeacct.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\inetcomm.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\oleacc.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\esent.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\ws2_32.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\nsi.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msidcrl30.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\SensApi.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\oleaccrc.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\INETRES.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\ACCTRES.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\psapi.dll
00:01:03	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Fonts\simhei.ttf

Unexpected Activities By Time (69 out of 89)

Elapsed Time	Type	Action
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\mlang.dll
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\drivers\mpsdrv.sys
00:01:04	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\$Mft
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\en-US\ESENT.dll.mui
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Fonts\upcll.ttf
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Users\admin\AppData\Local\Microsoft\Windows Mail\edb.log
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Fonts\constani.ttf
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Fonts\Candara.ttf
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files\Windows Mail\msoe.dll
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msident.dll
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Fonts\georgiai.ttf
00:01:04	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\$Mft
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Users\admin\AppData\Local\Microsoft\Windows Mail\WindowsMail.MSMessageStore
00:01:04	Registry Set	C:\Windows\System32\taskhost.exe **Set** HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}
00:01:04	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\$Mft

Unexpected Activities By Time (70 out of 89)

Elapsed Time	Type	Action
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\pstorec.dll
00:01:04	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Users\admin\AppData\Local\Microsoft\Windows Mail\WindowsMail.pat
00:01:04	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Program Files\Windows Mail\WinMail.exe
00:01:04	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\kernel32.dll
00:01:04	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\apisetschema.dll
00:01:04	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\KernelBase.dll
00:01:04	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\advapi32.dll
00:01:04	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msvcrt.dll
00:01:04	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\sechost.dll
00:01:04	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\rpcrt4.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\user32.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\gdi32.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\lpk.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\usp10.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msoert2.dll

Unexpected Activities By Time (71 out of 89)

Elapsed Time	Type	Action
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\ole32.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\oleaut32.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\shlwapi.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\shell32.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msctf.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\cryptbase.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\uxtheme.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Fonts\plantc.ttf
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\cryptdlg.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\wintrust.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Program Files\Windows Mail\msoe.dll
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Fonts\Candara.ttf
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Fonts\constani.ttf
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Fonts\georgiai.ttf

Unexpected Activities By Time (72 out of 89)

Elapsed Time	Type	Action
00:01:05	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Fonts\ntailu.ttf
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Fonts\nyala.ttf
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Fonts\phagspa.ttf
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Fonts\phagspab.ttf
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Fonts\simfang.ttf
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Fonts\simhei.ttf
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\Fonts\upcll.ttf
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Users\admin\AppData\Local\Temp\admin.bmp
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\ACCTRES.dll
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\atl.dll
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\clbcatq.dll
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\crypt32.dll
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\cryptsp.dll
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\cryptui.dll
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\esent.dll

Unexpected Activities By Time (73 out of 89)

Elapsed Time	Type	Action
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\iertutil.dll
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\imagehlp.dll
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\inetcomm.dll
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\INETRES.dll
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\mlang.dll
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msasn1.dll
00:01:06	Registry Set	C:\Windows\System32\taskhost.exe **Set** HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msftedit.dll
00:01:06	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msidcrl30.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msident.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msimg32.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msoeacct.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msxml6.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\normaliz.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\nsi.dll

Unexpected Activities By Time (74 out of 89)

Elapsed Time	Type	Action
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\oleacc.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\profapi.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\propsys.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\psapi.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\pstorec.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\RpcRtRemote.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\samlib.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\secur32.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\SensApi.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\shacct.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Program Files\Common Files\System\wab32res.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\sspicli.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\urlmon.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\wininet.dll
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\ws2_32.dll

Unexpected Activities By Time (75 out of 89)

Elapsed Time	Type	Action
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\drivers\mpsdrv.sys
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\en-US\ESENT.dll.mui
00:01:07	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7600.16385_none_72fc7cbf861225ca\GdiPlus.dll
00:01:08	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Users\admin\AppData\Local\Microsoft\Windows Mail\WindowsMail.pat
00:01:08	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Users\admin\AppData\Local\Microsoft\Windows Mail\edb.log
00:01:08	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Users\admin\AppData\Local\Microsoft\Windows Mail\WindowsMail.MSMessageStore
00:01:08	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msident.dll
00:01:08	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\pstorec.dll
00:01:08	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Program Files\Windows Mail\WinMail.exe
00:01:08	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Program Files\Windows Mail\msoe.dll
00:01:08	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\esent.dll
00:01:08	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\inetcomm.dll
00:01:08	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\mlang.dll
00:01:08	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msident.dll
00:01:08	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled

Unexpected Activities By Time (76 out of 89)

Elapsed Time	Type	Action
00:01:08	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers
00:01:08	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
00:01:08	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Session Manager\SafeDllSearchMode
00:01:08	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
00:01:09	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32\WinMail
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKCU
00:01:09	Registry Enumerate	C:\Program Files\Windows Mail\WinMail.exe **Enumerate** HKCU\Control Panel\Desktop\LanguageConfiguration
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKCU\Control Panel\Desktop\LanguageConfiguration
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKCU
00:01:09	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKCU\Control Panel\Desktop\PreferredUILanguages
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKCU\Control Panel\Desktop
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKCU
00:01:09	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKCU\Control Panel\Desktop\MuiCached\MachinePreferredUILanguages

Unexpected Activities By Time (77 out of 89)

Elapsed Time	Type	Action
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKCU\Control Panel\Desktop\MuiCached
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKCU
00:01:09	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\CMF\Config\SYSTEM
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\CMF\Config
00:01:09	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
00:01:09	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorUseSystemHeap
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\Ole
00:01:09	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorSystemHeapIsPrivate
00:01:09	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\Ole
00:01:09	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
00:01:10	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide
00:01:10	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
00:01:10	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide
00:01:10	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US

Unexpected Activities By Time (78 out of 89)

Elapsed Time	Type	Action
00:01:10	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale
00:01:10	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
00:01:10	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale
00:01:10	Registry Set	C:\Windows\System32\taskhost.exe **Set** HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}
00:01:10	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
00:01:10	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide
00:01:10	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKCU\Software\Microsoft\Internet Explorer\International\JP_ISO_SIO_Control
00:01:10	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKCU\Software\Microsoft\Internet Explorer\International
00:01:10	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
00:01:10	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide
00:01:10	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
00:01:10	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
00:01:10	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
00:01:10	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SYSTEM\ControlSet001\services\crypt32
00:01:10	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck

Unexpected Activities By Time (79 out of 89)

Elapsed Time	Type	Action
00:01:10	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
00:01:10	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
00:01:10	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
00:01:11	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
00:01:11	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\SQMClient\Windows
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\Ole\MaxSxSHashCount
00:01:11	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\Ole
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Microsoft\COM3\Com+Enabled
00:01:11	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Microsoft\COM3
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Read** HKCR
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Read** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Read** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}

Unexpected Activities By Time (80 out of 89)

Elapsed Time	Type	Action
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Read** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Read** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32\InprocServer32
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Read** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:11	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Read** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:12	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:12	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Read** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:12	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:12	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Read** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:12	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32\ThreadingModel
00:01:12	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:12	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Read** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:12	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}

Unexpected Activities By Time (81 out of 89)

Elapsed Time	Type	Action
00:01:12	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Read** HKCR
00:01:12	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKCR
00:01:12	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Read** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:12	Registry Close	C:\Program Files\Windows Mail\WinMail.exe **Closed** HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:12	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\msxml6.dll
00:01:12	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Windows\System32\pstorec.dll
00:01:12	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Program Files\Common Files\System\wab32res.dll
00:01:12	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Program Files\Common Files\System\wab32.dll
00:01:12	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32
00:01:12	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\sechost.dll
00:01:12	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msoert2.dll
00:01:13	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
00:01:13	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll
00:01:13	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\imm32.dll
00:01:13	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files\Windows Mail\en-US\WinMail.exe.mui

Unexpected Activities By Time (82 out of 89)

Elapsed Time	Type	Action
00:01:13	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\WindowsShell.Manifest
00:01:13	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
00:01:13	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\WindowsShell.Manifest
00:01:13	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\Globalization\Sorting\SortDefault.nls
00:01:13	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files\Windows Mail\msoe.dll
00:01:13	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\atl.dll
00:01:13	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msoeacct.dll
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\inetcomm.dll
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\oleacc.dll
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\uxtheme.dll
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\esent.dll
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msimg32.dll
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\propsys.dll
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\msidcrl30.dll
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\SensApi.dll

Unexpected Activities By Time (83 out of 89)

Elapsed Time	Type	Action
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\oleaccrc.dll
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\WindowsShell.Manifest
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\INETRES.dll
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\WindowsShell.Manifest
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\ACCTRES.dll
00:01:14	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\WindowsShell.Manifest
00:01:15	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
00:01:15	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Program Files\Windows Mail\MSOERES.dll
00:01:15	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\rpcss.dll
00:01:15	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\cryptbase.dll
00:01:15	File Modify	C:\Program Files\Windows Mail\WinMail.exe **Read From** C:\Program Files\Windows Mail\msoe.dll
00:01:15	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\mlang.dll
00:01:15	File Open	C:\Program Files\Windows Mail\WinMail.exe **Opened** C:\Windows\System32\en-US\mlang.dll.mui

Unexpected Activities By Time (84 out of 89)

89

Elapsed Time	Type	Action
00:01:15	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:15	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\864
00:01:15	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:15	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\708
00:01:15	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:15	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\708
00:01:15	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:15	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\51256
00:01:15	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\720
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\720
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\28596
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256

Unexpected Activities By Time (85 out of 89)

Elapsed Time	Type	Action
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\10004
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\50001
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1257
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\775
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1257
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\28594
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1257
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\28594
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1257
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1250
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\852
00:01:16	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1250
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\28592
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1250

Unexpected Activities By Time (86 out of 89)

Elapsed Time	Type	Action
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\10029
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1250
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\50936
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\51936
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\54936
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\20936
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\52936
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\50227
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936

Unexpected Activities By Time (87 out of 89)

Elapsed Time	Type	Action
00:01:17	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\10008
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\950
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\50950
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\950
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\20000
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\950
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\20002
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\950
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\50229
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\950
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\10002
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1250
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\10082
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\51251

Unexpected Activities By Time (88 out of 89)

Elapsed Time	Type	Action
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\866
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\28595
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:18	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\20866
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\21866
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\21866
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\10007
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1257
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\28603

Unexpected Activities By Time (89 out of 89)

Elapsed Time	Type	Action
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\29001
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\21027
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\863
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\20106
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1253
00:01:19	Registry Query	C:\Program Files\Windows Mail\WinMail.exe **Queried** HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\51253

Unexpected File System Activity (1 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:00:19	C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE	Create	C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:19	C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE	Write	C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Read	C:\$Directory
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\winspool.drv
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\apphelp.dll
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\AppPatch\sysmain.sdb
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Local
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Local\Temp
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\imm32.dll

Unexpected File System Activity (2 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\sechost.dll
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\secur32.dll
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\sspicli.dll
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\netapi32.dll
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\netutils.dll
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\srvcli.dll
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\wkscli.dll
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\samcli.dll
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\IPHLPAPI.DLL
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\winnsi.dll
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\version.dll
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\Globalization\Sorting\SortDefault.nls
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Roaming
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\profapi.dll

Unexpected File System Activity (3 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\LocalLow
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Read	C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Read	C:\$Mft
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Create	C:\Users\admin\AppData\Roaming\Uceso
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Read	C:\$Mft
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Create	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\cryptsp.dll
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\rsaenh.dll
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\cryptbase.dll
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Read	C:\$Directory
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Read	C:\$Mft
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Create	C:\Users\admin\AppData\LocalLow\ofukd.ism
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\LocalLow

Unexpected File System Activity (4 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Read	C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Delete	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Create	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Write	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Roaming
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Roaming\Uceso
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Roaming
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Write	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\System32\apphelp.dll
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\AppPatch\sysmain.sdb
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Roaming\Uceso

Unexpected File System Activity (5 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Roaming
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Roaming\Uceso
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Read	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Open	C:\Windows\AppPatch\sysmain.sdb
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Read	C:\$Directory
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Users\admin\AppData\Roaming
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\winspool.drv
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\apphelp.dll
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\AppPatch\sysmain.sdb

Unexpected File System Activity (6 out of 26)

100

Elapsed Time	Process Path	Activity	File Path
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Users
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Users\admin
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Users\admin\AppData
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Users\admin\AppData\Roaming
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Users\admin\AppData\Roaming\Uceso
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\imm32.dll
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\sechost.dll
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\secur32.dll
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\sspicli.dll
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\netapi32.dll
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\netutils.dll
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\srvcli.dll
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\wkscli.dll

Unexpected File System Activity (7 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\samcli.dll
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\IPHLPAPI.DLL
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\winnsi.dll
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\version.dll
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\Globalization\Sorting\SortDefault.nls
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Users\admin\AppData\Roaming
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Windows\System32\profapi.dll
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Users\admin\AppData\LocalLow
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Open	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Read	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32\secur32.dll
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32\sspicli.dll
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32\netapi32.dll
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32\netutils.dll

Unexpected File System Activity (8 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32\srvcli.dll
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32\wkscli.dll
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32\samcli.dll
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32\IPHLPAPI.DLL
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32\winnsi.dll
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32\dwm.exe
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32\userenv.dll
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Windows\System32\profapi.dll
00:00:58	C:\Windows\System32\dwm.exe	Read	C:\$Mft
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Users\admin\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates
00:00:58	C:\Windows\System32\dwm.exe	Read	C:\$Mft
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Users\admin\AppData\Roaming\Microsoft\SystemCertificates\My\CRLs
00:00:58	C:\Windows\System32\dwm.exe	Read	C:\$Mft
00:00:58	C:\Windows\System32\dwm.exe	Open	C:\Users\admin\AppData\Roaming\Microsoft\SystemCertificates\My\CTLs

Unexpected File System Activity (9 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\$Mft
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Prefetch\WINMAIL.EXE-1092D371.pf
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Prefetch\WINMAIL.EXE-1092D371.pf
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\$Mft
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\$EXTEND
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files\Common Files
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files\Common Files\System
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files\Windows Mail
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files\Windows Mail\en-US
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\ProgramData
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\ProgramData\Microsoft
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\ProgramData\Microsoft\User Account Pictures
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Users

Unexpected File System Activity (10 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Users\admin
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Users\admin\AppData
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Users\admin\AppData\Local
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Users\admin\AppData\Local\Microsoft
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\$Mft
00:00:59	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Users\admin\AppData\Local\Microsoft\Windows Mail
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Users\admin\AppData\Local\Microsoft\Windows Mail
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Users\admin\AppData\Local\Temp
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Fonts
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Fonts
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Globalization
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Globalization\Sorting
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\inf
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\inf

Unexpected File System Activity (11 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\drivers
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\drivers
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\en-US
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\en-US
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7600.16385_none_72fc7cbf861225ca
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\ntdll.dll
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files\Windows Mail\WinMail.exe
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\kernel32.dll
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\apisetschema.dll
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\KernelBase.dll
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\locale.nls
00:01:00	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\advapi32.dll

Unexpected File System Activity (12 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msvcrt.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\sechost.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\rpcrt4.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\user32.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\gdi32.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\lpk.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\usp10.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msoert2.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\ole32.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\oleaut32.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\shlwapi.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\shell32.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\imm32.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msctf.dll

Unexpected File System Activity (13 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files\Windows Mail\en-US\WinMail.exe.mui
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\WindowsShell.Manifest
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Globalization\Sorting\SortDefault.nls
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\rpcss.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\cryptbase.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\uxtheme.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Fonts\plantc.ttf
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\cryptdlg.dll
00:01:01	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\wintrust.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\crypt32.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msasn1.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\cryptui.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\imagehlp.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msimg32.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\secur32.dll

Unexpected File System Activity (14 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\sspicli.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\wininet.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\normaliz.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\urlmon.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\iertutil.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msftedit.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Fonts\phagspab.ttf
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Fonts\simfang.ttf
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\profapi.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\propsys.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\clbcatq.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Fonts\phagspa.ttf
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\cryptsp.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\rsaenh.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\RpcRtRemote.dll

Unexpected File System Activity (15 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files\Common Files\System\wab32.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msxml6.dll
00:01:02	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\en-US\KernelBase.dll.mui
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msxml6r.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Fonts\nyala.ttf
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7600.16385_none_72fc7cbf861225ca\GdiPlus.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files\Common Files\System\wab32res.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\shacct.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\samlib.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\ProgramData\Microsoft\User Account Pictures\user.bmp
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Users\admin\AppData\Local\Temp\admin.bmp
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Fonts\ntailu.ttf
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\atl.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msoeacct.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\inetcomm.dll

Unexpected File System Activity (16 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\oleacc.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\esent.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\ws2_32.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\nsi.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msidcrl30.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\SensApi.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\oleaccrc.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\INETRES.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\ACCTRES.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\psapi.dll
00:01:03	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Fonts\simhei.ttf
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\mlang.dll
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\drivers\mpsdrv.sys
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\$Mft
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\en-US\ESENT.dll.mui

Unexpected File System Activity (17 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Fonts\upcll.ttf
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Users\admin\AppData\Local\Microsoft\Windows Mail\edb.log
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Fonts\constani.ttf
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Fonts\Candara.ttf
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files\Windows Mail\msoe.dll
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msident.dll
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Fonts\georgiai.ttf
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\$Mft
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Users\admin\AppData\Local\Microsoft\Windows Mail\WindowsMail.MSMessageStore
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\$Mft
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\pstorec.dll
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Users\admin\AppData\Local\Microsoft\Windows Mail\WindowsMail.pat
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Program Files\Windows Mail\WinMail.exe
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\kernel32.dll
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\apisetschema.dll

Unexpected File System Activity (18 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\KernelBase.dll
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\advapi32.dll
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msvcrt.dll
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\sechost.dll
00:01:04	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\rpcrt4.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\user32.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\gdi32.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\lpk.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\usp10.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msoert2.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\ole32.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\oleaut32.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\shlwapi.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\shell32.dll

Unexpected File System Activity (19 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msctf.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\cryptbase.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\uxtheme.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Fonts\plantc.ttf
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\cryptdlg.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\wintrust.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Program Files\Windows Mail\msoe.dll
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Fonts\Candara.ttf
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Fonts\constani.ttf
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Fonts\georgiai.ttf
00:01:05	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Fonts\ntailu.ttf
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Fonts\nyala.ttf
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Fonts\phagspa.ttf
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Fonts\phagspab.ttf
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Fonts\simfang.ttf

Unexpected File System Activity (20 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Fonts\simhei.ttf
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\Fonts\upcll.ttf
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Users\admin\AppData\Local\Temp\admin.bmp
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\ACCTRES.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\atl.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\clbcatq.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\crypt32.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\cryptsp.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\cryptui.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\esent.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\iertutil.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\imagehlp.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\inetcomm.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\INETRES.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\mlang.dll

Unexpected File System Activity (21 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msasn1.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msftedit.dll
00:01:06	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msidcrl30.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msident.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msimg32.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msoeacct.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msxml6.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\normaliz.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\nsi.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\oleacc.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\profapi.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\propsys.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\psapi.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\pstorec.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\RpcRtRemote.dll

Unexpected File System Activity (22 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\samlib.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\secur32.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\SensApi.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\shacct.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Program Files\Common Files\System\wab32res.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\sspicli.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\urlmon.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\wininet.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\ws2_32.dll
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\drivers\mpsdrv.sys
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\en-US\ESENT.dll.mui
00:01:07	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\winsxs\x86_microsoft.windows.gdiplus_6595b64144ccf1df_1.1.7600.16385_none_72fc7cbf861225ca\GdiPlus.dll
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Users\admin\AppData\Local\Microsoft\Windows Mail\WindowsMail.pat
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Users\admin\AppData\Local\Microsoft\Windows Mail\edb.log
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Users\admin\AppData\Local\Microsoft\Windows Mail\WindowsMail.MSMessageStore

Unexpected File System Activity (23 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msident.dll
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\pstorec.dll
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Program Files\Windows Mail\WinMail.exe
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Program Files\Windows Mail\msoe.dll
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\esent.dll
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\inetcomm.dll
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\mlang.dll
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msident.dll
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\msxml6.dll
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Windows\System32\pstorec.dll
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Program Files\Common Files\System\wab32res.dll
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Program Files\Common Files\System\wab32.dll
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\sechost.dll
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msoert2.dll

Unexpected File System Activity (24 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:13	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
00:01:13	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc\comctl32.dll
00:01:13	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\imm32.dll
00:01:13	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files\Windows Mail\en-US\WinMail.exe.mui
00:01:13	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\WindowsShell.Manifest
00:01:13	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
00:01:13	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\WindowsShell.Manifest
00:01:13	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\Globalization\Sorting\SortDefault.nls
00:01:13	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files\Windows Mail\msoe.dll
00:01:13	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\atl.dll
00:01:13	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msoeacct.dll
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\inetcomm.dll
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\oleacc.dll
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\uxtheme.dll
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\esent.dll

Unexpected File System Activity (25 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msimg32.dll
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\propsys.dll
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\msidcrl30.dll
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\SensApi.dll
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\oleaccrc.dll
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\WindowsShell.Manifest
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\INETRES.dll
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\WindowsShell.Manifest
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\ACCTRES.dll
00:01:14	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\WindowsShell.Manifest
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7600.16385_none_421189da2b7fabfc
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Program Files\Windows Mail\MSOERES.dll
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\rpcss.dll

Unexpected File System Activity (26 out of 26)

Elapsed Time	Process Path	Activity	File Path
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\cryptbase.dll
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Read	C:\Program Files\Windows Mail\msoe.dll
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\mlang.dll
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Open	C:\Windows\System32\en-US\mlang.dll.mui

Attempted Network Connections

121

No data found

Unexpected Process Activity

122

Elapsed Time	Process Path	Activity	Target Process
00:00:19	C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE	Create	C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:19	C:\Program Files\Microsoft Office\OFFICE11\WINWORD.EXE	Create	C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Create	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:59	C:\Windows\System32\svchost.exe	Create	C:\Program Files\Windows Mail\WinMail.exe

Unexpected Registry Activity (1 out of 63)

123

Elapsed Time	Process Path	Activity	Registry Key
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Terminal Server\TSAppCompat
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Terminal Server\TSUserEnabled
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\Control\Terminal Server
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\ShowDebugInfo
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\admin\AppData\Local\Temp\paw.exe
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Session Manager\SafeDllSearchMode
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize

Unexpected Registry Activity (2 out of 63)

124

Elapsed Time	Process Path	Activity	Registry Key
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32\paw
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Enumerate	HKCU\Control Panel\Desktop\LanguageConfiguration
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU\Control Panel\Desktop\LanguageConfiguration
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKCU\Control Panel\Desktop\PreferredUILanguages
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU\Control Panel\Desktop
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKCU\Control Panel\Desktop\MuiCached\MachinePreferredUILanguages
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU\Control Panel\Desktop\MuiCached
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorUseSystemHeap

Unexpected Registry Activity (3 out of 63)

125

Elapsed Time	Process Path	Activity	Registry Key
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Ole
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorSystemHeapIsPrivate
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Ole
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\crypt32
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters\RpcCacheTimeout
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\SQMClient\Windows
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\WinSock_Registry_Version
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US

Unexpected Registry Activity (4 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\AppId_Catalog
00:00:30	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Callout
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Serial_Access_Num
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Next_Catalog_Entry_ID
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Num_Catalog_Entries
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004\PackedCatalogItem

Unexpected Registry Activity (5 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011

Unexpected Registry Activity (6 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000014\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000014
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000015\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000015
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000016\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000016
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000017\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000017
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018\PackedCatalogItem
00:00:31	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000019\PackedCatalogItem

Unexpected Registry Activity (7 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000019
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000020\PackedCatalogItem
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000020
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000021\PackedCatalogItem
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000021
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000022\PackedCatalogItem
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000022
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000023\PackedCatalogItem
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000023
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000024\PackedCatalogItem
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000024
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Serial_Access_Num
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Num_Catalog_Entries
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\LibraryPath

Unexpected Registry Activity (8 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\DisplayString
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\ProviderId
00:00:32	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\AddressFamily
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\SupportedNameSpace
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\Enabled
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\Version
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\StoresServiceClassInfo
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\ProviderInfo
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\LibraryPath
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\DisplayString
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\ProviderId
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\AddressFamily
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\SupportedNameSpace
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\Enabled

Unexpected Registry Activity (9 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\Version
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\StoresServiceClassInfo
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\ProviderInfo
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\LibraryPath
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\DisplayString
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\ProviderId
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\AddressFamily
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\SupportedNameSpace
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\Enabled
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\Version
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\StoresServiceClassInfo
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\ProviderInfo
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\LibraryPath

Unexpected Registry Activity (10 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\DisplayString
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\ProviderId
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\AddressFamily
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\SupportedNameSpace
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\Enabled
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\Version
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\StoresServiceClassInfo
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\ProviderInfo
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\LibraryPath
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\DisplayString
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\ProviderId
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\AddressFamily
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\SupportedNameSpace
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\Enabled

Unexpected Registry Activity (11 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\Version
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\StoresServiceClassInfo
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\ProviderInfo
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\LibraryPath
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\DisplayString
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\ProviderId
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\AddressFamily
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\SupportedNameSpace
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\Enabled
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\Version
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\StoresServiceClassInfo
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\ProviderInfo
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries

Unexpected Registry Activity (12 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Ws2_32NumHandleBuckets
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Rpc\MaxRpcSize
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Rpc
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName\ComputerName
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\Setup\OOBEInProgress
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\Setup
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\Setup\SystemSetupInProgress
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\Setup
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\SQMClient\Windows
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Category

Unexpected Registry Activity (13 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Name
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\ParentFolder
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Description
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\RelativePath
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\ParsingName
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\InfoTip
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\LocalizedName
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Icon
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Security
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\StreamResource
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\StreamResourceType
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\LocalRedirectOnly
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Roamable
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PreCreate
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Stream

Unexpected Registry Activity (14 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PublishExpandedPath
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Attributes
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\FolderTypeID
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\InitFolderHandler
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Category
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Name
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\ParentFolder
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Description
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\RelativePath
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\ParsingName
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\InfoTip
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\LocalizedName
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Icon

Unexpected Registry Activity (15 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Security
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\StreamResource
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\StreamResourceType
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\LocalRedirectOnly
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Roamable
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\PreCreate
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Stream
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\PublishExpandedPath
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Attributes
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\FolderTypeID
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\InitFolderHandler
00:00:37	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData

Unexpected Registry Activity (16 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Category
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Name
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\ParentFolder
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Description
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\RelativePath
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\ParsingName
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\InfoTip
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\LocalizedName
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Icon
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Security
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\StreamResource
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\StreamResourceType
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\LocalRedirectOnly

Unexpected Registry Activity (17 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Roamable
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\PreCreate
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Stream
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\PublishExpandedPath
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Attributes
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\FolderTypeID
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\InitFolderHandler
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\{A520A1A4-1780-4FF6-BD18-167343C5AF16}
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Category
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Name
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParentFolder

Unexpected Registry Activity (18 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Description
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\RelativePath
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParsingName
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InfoTip
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalizedName
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Icon
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Security
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResource
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResourceType
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalRedirectOnly
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Roamable
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PreCreate
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Stream
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PublishExpandedPath
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Attributes

Unexpected Registry Activity (19 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\FolderTypeID
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InitFolderHandler
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-292738990-2461527479-3432112557-1000\ProfileImagePath
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-292738990-2461527479-3432112557-1000
00:00:38	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU\Software\Microsoft\Keyvb
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU\Software\Microsoft
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName\ComputerName
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\Setup\OOBEInProgress
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\Setup
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\Setup\SystemSetupInProgress
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\Setup
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\Control\ComputerName

Unexpected Registry Activity (20 out of 63)

142

Elapsed Time	Process Path	Activity	Registry Key
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate
00:00:39	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DigitalProductId
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced Cryptographic Provider v1.0\Type
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced Cryptographic Provider v1.0\Image Path
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Session Manager\SafeProcessSearchMode
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy\Enabled
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SYSTEM\ControlSet001\Control\Lsa
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Policies\Microsoft\Cryptography\PrivKeyCacheMaxItems
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Policies\Microsoft\Cryptography\PrivKeyCachePurgeIntervalSeconds
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Policies\Microsoft\Cryptography\PrivateKeyLifetimeSeconds
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Policies\Microsoft\Cryptography
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Cryptography\MachineGuid

Unexpected Registry Activity (21 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Cryptography
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Cryptography\Defaults\Provider\Microsoft Enhanced Cryptographic Provider v1.0
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\AuthenticodeEnabled
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\DisableLocalOverride
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
00:00:40	C:\Users\admin\AppData\Local\Temp\paw.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Terminal Server\TSAppCompat
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Terminal Server\TSUserEnabled
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\Control\Terminal Server

Unexpected Registry Activity (22 out of 63)

144

Elapsed Time	Process Path	Activity	Registry Key
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\ShowDebugInfo
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\Cache
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers\C:\Users\admin\AppData\Roaming\Uceso\uppu.exe
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Session Manager\SafeDllSearchMode
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
00:00:40	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32\uppu
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU

Unexpected Registry Activity (23 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Enumerate	HKCU\Control Panel\Desktop\LanguageConfiguration
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU\Control Panel\Desktop\LanguageConfiguration
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKCU\Control Panel\Desktop\PreferredUILanguages
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU\Control Panel\Desktop
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKCU\Control Panel\Desktop\MuiCached\MachinePreferredUILanguages
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU\Control Panel\Desktop\MuiCached
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorUseSystemHeap
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Ole
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorSystemHeapIsPrivate
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Ole

Unexpected Registry Activity (24 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\crypt32
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
00:00:41	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters\RpcCacheTimeout
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\SQMClient\Windows
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\WinSock_Registry_Version
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale

Unexpected Registry Activity (25 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\AppId_Catalog
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Callout
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Serial_Access_Num
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Next_Catalog_Entry_ID
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Num_Catalog_Entries
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001\PackedCatalogItem
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002\PackedCatalogItem
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003\PackedCatalogItem
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004\PackedCatalogItem
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005\PackedCatalogItem
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005

Unexpected Registry Activity (26 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006\PackedCatalogItem
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007\PackedCatalogItem
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008\PackedCatalogItem
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009\PackedCatalogItem
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010\PackedCatalogItem
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011\PackedCatalogItem
00:00:42	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012\PackedCatalogItem
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013\PackedCatalogItem

Unexpected Registry Activity (27 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000014\PackedCatalogItem
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000014
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000015\PackedCatalogItem
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000015
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000016\PackedCatalogItem
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000016
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000017\PackedCatalogItem
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000017
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018\PackedCatalogItem
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000019\PackedCatalogItem
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000019
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000020\PackedCatalogItem
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000020

Unexpected Registry Activity (28 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000021\PackedCatalogItem
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000021
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000022\PackedCatalogItem
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000022
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000023\PackedCatalogItem
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000023
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000024\PackedCatalogItem
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000024
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Serial_Access_Num
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Num_Catalog_Entries
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\LibraryPath
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\DisplayString
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\ProviderId
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\AddressFamily

Unexpected Registry Activity (29 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\SupportedNameSpace
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\Enabled
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\Version
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\StoresServiceClassInfo
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\ProviderInfo
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\LibraryPath
00:00:43	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\DisplayString
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\ProviderId
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\AddressFamily
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\SupportedNameSpace
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\Enabled
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\Version
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\StoresServiceClassInfo
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\ProviderInfo

Unexpected Registry Activity (30 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\LibraryPath
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\DisplayString
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\ProviderId
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\AddressFamily
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\SupportedNameSpace
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\Enabled
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\Version
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\StoresServiceClassInfo
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\ProviderInfo
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\LibraryPath
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\DisplayString
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\ProviderId
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\AddressFamily

Unexpected Registry Activity (31 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\SupportedNameSpace
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\Enabled
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\Version
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\StoresServiceClassInfo
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\ProviderInfo
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\LibraryPath
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\DisplayString
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\ProviderId
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\AddressFamily
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\SupportedNameSpace
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\Enabled
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\Version
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\StoresServiceClassInfo
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\ProviderInfo

Unexpected Registry Activity (32 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\LibraryPath
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\DisplayString
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\ProviderId
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\AddressFamily
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\SupportedNameSpace
00:00:44	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\Enabled
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\Version
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\StoresServiceClassInfo
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\ProviderInfo
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Ws2_32NumHandleBuckets
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters

Unexpected Registry Activity (33 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Rpc\MaxRpcSize
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Rpc
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName\ComputerName
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\Setup\OOBEInProgress
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\Setup
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SYSTEM\Setup\SystemSetupInProgress
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SYSTEM\Setup
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\SQMClient\Windows
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Category
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Name
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\ParentFolder
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Description

Unexpected Registry Activity (34 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\RelativePath
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\ParsingName
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\InfoTip
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\LocalizedName
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Icon
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Security
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\StreamResource
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\StreamResourceType
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\LocalRedirectOnly
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Roamable
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PreCreate
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Stream
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\PublishExpandedPath
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\Attributes
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\FolderTypeID

Unexpected Registry Activity (35 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}\InitFolderHandler
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{F38BF404-1D43-42F2-9305-67DE0B28FC23}
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Category
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Name
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\ParentFolder
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Description
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\RelativePath
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\ParsingName
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\InfoTip
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\LocalizedName
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Icon
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Security
00:00:45	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\StreamResource
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\StreamResourceType

Unexpected Registry Activity (36 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\LocalRedirectOnly
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Roamable
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\PreCreate
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Stream
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\PublishExpandedPath
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\Attributes
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\FolderTypeID
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}\InitFolderHandler
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{3EB685DB-65F9-4CF6-A03A-E3EF65729F3D}
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\AppData
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Category

Unexpected Registry Activity (37 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Name
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\ParentFolder
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Description
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\RelativePath
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\ParsingName
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\InfoTip
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\LocalizedName
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Icon
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Security
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\StreamResource
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\StreamResourceType
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\LocalRedirectOnly
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Roamable
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\PreCreate
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Stream

Unexpected Registry Activity (38 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:46	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\PublishExpandedPath
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\Attributes
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\FolderTypeID
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}\InitFolderHandler
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{A520A1A4-1780-4FF6-BD18-167343C5AF16}
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\{A520A1A4-1780-4FF6-BD18-167343C5AF16}
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Category
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Name
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParentFolder
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Description
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\RelativePath
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\ParsingName

Unexpected Registry Activity (39 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InfoTip
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalizedName
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Icon
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Security
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResource
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\StreamResourceType
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\LocalRedirectOnly
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Roamable
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PreCreate
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Stream
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\PublishExpandedPath
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\Attributes
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\FolderTypeID
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}\InitFolderHandler
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{5E6C858F-0E22-4760-9AFE-EA3317B67173}

Unexpected Registry Activity (40 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-292738990-2461527479-3432112557-1000\ProfileImagePath
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-292738990-2461527479-3432112557-1000
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKCU\Software\Microsoft\Keyvb\19bc8hhb
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU\Software\Microsoft\Keyvb
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Query	HKCU\Software\Microsoft\Keyvb\15fg6gj5
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU\Software\Microsoft\Keyvb
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Set	HKCU\Software\Microsoft\Keyvb\15fg6gj5
00:00:47	C:\Users\admin\AppData\Roaming\Uceso\uppu.exe	Close	HKCU\Software\Microsoft\Keyvb
00:00:52	C:\Windows\System32\taskhost.exe	Set	HKCU\Software\Microsoft\Keyvb\19bc8hhb
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters\RpcCacheTimeout

Unexpected Registry Activity (41 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\LanmanWorkstation\Parameters
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\WinSock_Registry_Version
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\AppId_Catalog
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Callout
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Serial_Access_Num
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Next_Catalog_Entry_ID
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Num_Catalog_Entries
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000001
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000002
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000003
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000004

Unexpected Registry Activity (42 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000005
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000006
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000007
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000008
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000009
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000010
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000011
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012\PackedCatalogItem

Unexpected Registry Activity (43 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000012
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000013
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000014\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000014
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000015\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000015
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000016\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000016
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000017\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000017
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000018
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000019\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000019

Unexpected Registry Activity (44 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000020\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000020
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000021\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000021
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000022\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000022
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000023\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000023
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000024\PackedCatalogItem
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries\000000000024
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Serial_Access_Num
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Num_Catalog_Entries
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\LibraryPath
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\DisplayString

Unexpected Registry Activity (45 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\ProviderId
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\AddressFamily
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\SupportedNameSpace
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\Enabled
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\Version
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\StoresServiceClassInfo
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001\ProviderInfo
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000001
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\LibraryPath
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\DisplayString
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\ProviderId
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\AddressFamily
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\SupportedNameSpace
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\Enabled
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\Version

Unexpected Registry Activity (46 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\StoresServiceClassInfo
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002\ProviderInfo
00:00:52	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000002
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\LibraryPath
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\DisplayString
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\ProviderId
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\AddressFamily
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\SupportedNameSpace
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\Enabled
00:00:52	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\Version
00:00:53	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\StoresServiceClassInfo
00:00:53	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003\ProviderInfo
00:00:53	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000003
00:00:53	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\LibraryPath
00:00:53	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\DisplayString

Unexpected Registry Activity (47 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\ProviderId
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\AddressFamily
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\SupportedNameSpace
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\Enabled
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\Version
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\StoresServiceClassInfo
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004\ProviderInfo
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000004
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\LibraryPath
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\DisplayString
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\ProviderId
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\AddressFamily
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\SupportedNameSpace
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\Enabled
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\Version

Unexpected Registry Activity (48 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\StoresServiceClassInfo
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005\ProviderInfo
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000005
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\LibraryPath
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\DisplayString
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\ProviderId
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\AddressFamily
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\SupportedNameSpace
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\Enabled
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\Version
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\StoresServiceClassInfo
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006\ProviderInfo
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries\000000000006
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters

Unexpected Registry Activity (49 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters\Ws2_32NumHandleBuckets
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\WinSock2\Parameters
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Category
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Name
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\ParentFolder
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Description
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\RelativePath
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\ParsingName
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\InfoTip
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\LocalizedName
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Icon
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Security
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\StreamResource
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\StreamResourceType

Unexpected Registry Activity (50 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\LocalRedirectOnly
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Roamable
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\PreCreate
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Stream
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\PublishExpandedPath
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\Attributes
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\FolderTypeID
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\InitFolderHandler
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions\{1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}
00:00:58	C:\Windows\System32\dwm.exe	Query	HKCU\Software\Microsoft\Keyvb\19bc8hhb
00:00:58	C:\Windows\System32\dwm.exe	Close	HKCU\Software\Microsoft\Keyvb
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\crypt32\DiagLevel
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\crypt32\DiagMatchAnyMask
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\crypt32
00:00:58	C:\Windows\System32\dwm.exe	Enumerate	HKLM\SOFTWARE\Microsoft\Cryptography\OID

Unexpected Registry Activity (51 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:58	C:\Windows\System32\dwm.exe	Enumerate	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\#16
00:00:58	C:\Windows\System32\dwm.exe	Enumerate	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\#16
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\#16
00:00:58	C:\Windows\System32\dwm.exe	Enumerate	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\Ldap
00:00:58	C:\Windows\System32\dwm.exe	Enumerate	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\Ldap
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv\Ldap
00:00:58	C:\Windows\System32\dwm.exe	Enumerate	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CertDllOpenStoreProv
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0
00:00:58	C:\Windows\System32\dwm.exe	Enumerate	HKLM\SOFTWARE\Microsoft\Cryptography\OID
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 1
00:00:58	C:\Windows\System32\dwm.exe	Enumerate	HKLM\SOFTWARE\Microsoft\Cryptography\OID
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SOFTWARE\Microsoft\Cryptography\OID

Unexpected Registry Activity (52 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:00:58	C:\Windows\System32\dwm.exe	Close	HKCU
00:00:58	C:\Windows\System32\dwm.exe	Close	HKCU\Software\Microsoft\SystemCertificates\My
00:00:58	C:\Windows\System32\dwm.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-292738990-2461527479-3432112557-1000\ProfileImagePath
00:00:58	C:\Windows\System32\dwm.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\S-1-5-21-292738990-2461527479-3432112557-1000
00:00:58	C:\Windows\System32\dwm.exe	Close	HKCU
00:00:58	C:\Windows\System32\dwm.exe	Close	HKCU\Software\Microsoft\SystemCertificates\My
00:00:58	C:\Windows\System32\dwm.exe	Set	HKCU\Software\Microsoft\Keyvb\19bc8hhb
00:00:58	C:\Windows\System32\dwm.exe	Close	HKCU\Software\Microsoft\Keyvb
00:00:59	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\crypt32\DiagLevel
00:00:59	C:\Windows\System32\dwm.exe	Query	HKLM\SYSTEM\ControlSet001\services\crypt32\DiagMatchAnyMask
00:00:59	C:\Windows\System32\dwm.exe	Close	HKLM\SYSTEM\ControlSet001\services\crypt32
00:00:59	C:\Windows\System32\taskhost.exe	Set	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}
00:00:59	C:\Windows\System32\taskhost.exe	Delete Value	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\internat.exe
00:00:59	C:\Windows\System32\taskhost.exe	Set	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}
00:00:59	C:\Windows\System32\taskhost.exe	Set	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}

Unexpected Registry Activity (53 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:01:04	C:\Windows\System32\taskhost.exe	Set	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}
00:01:06	C:\Windows\System32\taskhost.exe	Set	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers\TransparentEnabled
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Session Manager\SafeDllSearchMode
00:01:08	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32\WinMail
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKCU
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Enumerate	HKCU\Control Panel\Desktop\LanguageConfiguration
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKCU\Control Panel\Desktop\LanguageConfiguration
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKCU
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Query	HKCU\Control Panel\Desktop\PreferredUILanguages

Unexpected Registry Activity (54 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKCU\Control Panel\Desktop
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKCU
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Query	HKCU\Control Panel\Desktop\MuiCached\MachinePreferredUILanguages
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKCU\Control Panel\Desktop\MuiCached
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKCU
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\CMF\Config\SYSTEM
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SYSTEM\ControlSet001\Control\CMF\Config
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\LoadAppInit_DLLs
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorUseSystemHeap
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\Ole
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\Ole\PageAllocatorSystemHeapIsPrivate
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\Ole
00:01:09	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide

Unexpected Registry Activity (55 out of 63)

177

Elapsed Time	Process Path	Activity	Registry Key
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SYSTEM\ControlSet001\Control\Nls\CustomLocale
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale
00:01:10	C:\Windows\System32\taskhost.exe	Set	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\{9439A768-4AC5-AD41-A646-4BEFAC9368F2}
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Query	HKCU\Software\Microsoft\Internet Explorer\International\JP_ISO_SIO_Control
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Close	HKCU\Software\Microsoft\Internet Explorer\International
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\Language Groups\1

Unexpected Registry Activity (56 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SYSTEM\ControlSet001\services\crypt32
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
00:01:10	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\SideBySide
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\SQMClient\Windows\CEIPEnable
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\SQMClient\Windows
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\Ole\MaxSxSHashCount
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\Ole
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Microsoft\COM3\Com+Enabled
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Microsoft\COM3
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKCR

Unexpected Registry Activity (57 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32\InprocServer32
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:11	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32\ThreadingModel

Unexpected Registry Activity (58 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}\InProcServer32
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Query	HKCR
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Close	HKCR
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:12	C:\Program Files\Windows Mail\WinMail.exe	Close	HKLM\SOFTWARE\Classes\CLSID\{275C23E2-3747-11D0-9FEA-00AA003F8646}
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\864
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\708
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\708
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\51256

Unexpected Registry Activity (59 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:01:15	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\720
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\720
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\28596
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\10004
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1256
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\50001
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1257
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\775
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1257
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\28594
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1257

Unexpected Registry Activity (60 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\28594
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1257
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1250
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\852
00:01:16	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1250
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\28592
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1250
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\10029
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1250
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\50936
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\51936
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\54936

Unexpected Registry Activity (61 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\20936
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\52936
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\50227
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\936
00:01:17	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\10008
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\950
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\50950
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\950
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\20000
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\950
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\20002
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\950

Unexpected Registry Activity (62 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\50229
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\950
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\10002
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1250
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\10082
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\51251
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\866
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\28595
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:18	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\20866
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\21866

Unexpected Registry Activity (63 out of 63)

Elapsed Time	Process Path	Activity	Registry Key
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\21866
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\10007
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1251
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1257
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\28603
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\29001
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\21027
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\863
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\20106
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\1253
00:01:19	C:\Program Files\Windows Mail\WinMail.exe	Query	HKLM\SYSTEM\ControlSet001\Control\Nls\CodePage\51253