Orion Malware Analysis Report

Version 4.4.0

Overview

Global Risk

Global risk level is evaluated from results on static and dynamic analysis in charge of detecting suspicious activities.

Risk	**High**
Warnings	• File type not supported by scanner analyzer

- ***Severe***: *Analysis engines are confident to define this data as a malware.*
- ***High***: *Analysis engines have detected high risk level activities usually used by malwares.*
- ***Medium***: *Analysis engines have detected suspicious activities. More investigation is recommended.*
- ***Low***: *Analysis engines have not detected any suspicious activity.*
- ***Safe***: *Analysis engines have recognized a trusted data.*
- ***N/A***: *Risk level cannot be evaluated on this file for different reasons: file type not supported, analyzers not available,...*

Identification

SHA256	9d3b5a6370f076a57651fcf06fc4f3fbce8d9e5156642e22141a8f521f35ffdc
File names	• Close Goose.bat
File type	Batch script, ASCII text, with no line terminators
Last updated (UTC)	Jul 21 07 2022 11:08:27
Start analysis (UTC)	Jul 21 07 2022 11:07:59
End analysis (UTC)	Jul 21 07 2022 11:08:27

Analysis workflow

Analyzers name	Reputation	Antivirus	Rules	Scanner	Dynamic
Enabled	Yes	Yes	Yes	Yes	Yes
Errors	-	-	-	['File type not supported by scanner analyzer']	-
Stopped early	-	-	-	-	-

Dynamic Environment

Operating System	Windows 7
Description	Windows 7 Pro SP1 64bits with Office Pro plus 2007, Chrome 66, IE 8, Adobe Reader 8, Java 8, OpenOffice 2.3, dotnet 3.5.1
Duration	120
Connected to Internet	False

Detected payloads

This section describes all analyzed payloads. A payload is a part of file that could contain suspicious activities. As example, a malicious Windows executable is detected as a payload of its dropper. Moreover all enclosed files of a compressed archive are detected as payloads.

To obtain more detail on a payload, please consult its analysis report

No payload has been detected

Reputation

This section indicate if the file has a matching entry in reputation database.

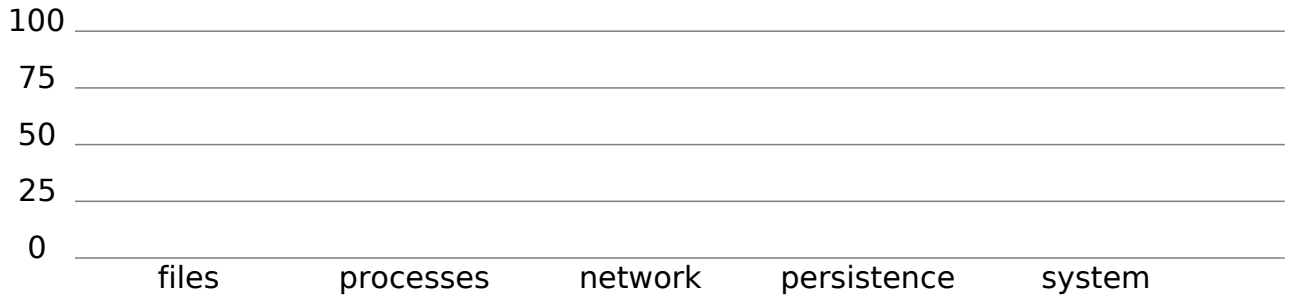
Risk of compromise

This section describes suspicious activities that have been detected on different type of activities as files, processes, network, persistence and system activities. For each type of activity a score level is evaluated between 0 to 100.

- *file activities: analysis has detected rules on file or detected suspicious activities on filesystem.*
- *processes activities: analysis has detected suspicous activities on processes such as file execution , injection into other process, ...*
- *network activities: analysis has detected network communications, found command and control server addresses,...*
- *persistence activities: analysis has detected a persistent installation. It means that the submitted file will remain active in the event of a reboot*
- *system activities: analysis has detected requests or modifications on system.*

Scanner Analysis

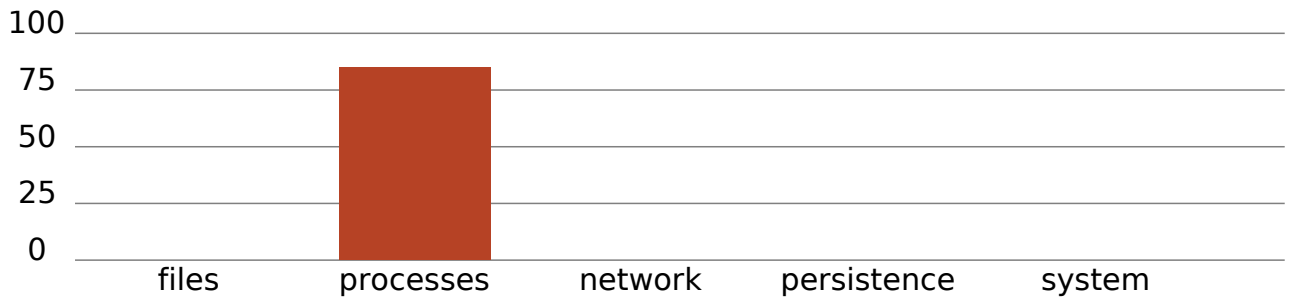
Suspicious activities that have been detected by scanner's analysis.



Type	Activities

Dynamic Analysis

Suspicious activities that have been detected by dynamic analysis.



Type	Activities
Process	• Creates processes • Kills process(es) during the analysis

MITRE ATT&CK Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
				T1562.001 - Disable or Modify Tools							

Static Analysis

This section details static analysis result.

Antivirus results

This section lists antivirus results on the subject.

0 / 4 Antivirus matched

Antivirus	Threat name	Engine version	Signatures version	Last update
Symantec	Clean	151.1.4.39	07/20/22 rev. 22	2022-07-21T03:36:56+00:00
Eset	Clean	7.2.574.0	20220210	2022-07-21T03:24:44+00:00
Avira	Clean	8.3.64.176	8.19.20.200	2022-07-21T03:31:00+00:00
Avast	Clean	3.0.3	22072004	2022-07-21T03:44:13+00:00

Matched rules

This section lists detection rules that have matched with the subject.

The rules are based on the the package created at Jun 17 06 2022 14:19:37 (UTC)

Scanner Analysis

Analyzer Information

Detection package version: 4.16

Dynamic Analysis

This section describes dynamic analysis results.

Analyzer Information

Detection package version: 4.16
Dynamic heuristics generated at: 2022-06-17 14:19:24.525000 (UTC)
Behavioral heuristics generated at: 2022-06-17 14:19:24.826000 (UTC)
OpenIOC rules generated at: 2022-06-17 14:19:37.614825 (UTC)

Matched rules

This section lists detection rules that have matched with the subject.

Network Activity

This section describes network activities detected by dynamic analysis.

Network connections

List of network connections (TCP, UDP, ICMP, ...) which have been detected during analysis.

IP Address	Port	Number of occurrences
<honeypot-dns>	137	1
<honeypot-dns>	138	1
<host-ip>	3	1

Processes tree

This tree shows relationship between parents and its child processes.

- **cmd.exe**
  - **taskkill.exe**

Dynamic Library Loads Activity

This sections shows attempts to load a dynamic library that may or may not be present on the system.

Analysis is based on files and memory mapping activities.

cmd.exe (PID:820)

Dynamic library loads activity for process cmd.exe (pid:820)

C:\Windows\SYSTEM32\wow64.dll
C:\Windows\SYSTEM32\wow64win.dll
C:\Windows\SYSTEM32\wow64cpu.dll
C:\Windows\syswow64\kernel32.dll

C:\Windows\syswow64\KERNELBASE.dll
C:\Windows\syswow64\msvcrt.dll
C:\Windows\syswow64\WINBRAND.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\syswow64\GDI32.dll
C:\Windows\syswow64\LPK.dll
C:\Windows\syswow64\USP10.dll
C:\Windows\syswow64\ADVAPI32.dll
C:\Windows\SysWOW64\sechost.dll
C:\Windows\syswow64\RPCRT4.dll
C:\Windows\syswow64\SspiCli.dll
C:\Windows\syswow64\CRYPTBASE.dll
C:\Windows\SysWOW64\IMM32.DLL
C:\Windows\syswow64\MSCTF.dll

taskkill.exe (PID:1268)

Dynamic library loads activity for process taskkill.exe (pid:1268)

C:\Windows\SYSTEM32\wow64.dll
C:\Windows\SYSTEM32\wow64win.dll
C:\Windows\SYSTEM32\wow64cpu.dll
C:\Windows\syswow64\kernel32.dll
C:\Windows\syswow64\KERNELBASE.dll
C:\Windows\syswow64\ADVAPI32.dll
C:\Windows\syswow64\msvcrt.dll
C:\Windows\SysWOW64\sechost.dll
C:\Windows\syswow64\RPCRT4.dll
C:\Windows\syswow64\SspiCli.dll
C:\Windows\syswow64\CRYPTBASE.dll
C:\Windows\SysWOW64\VERSION.dll
C:\Windows\syswow64\USER32.dll
C:\Windows\syswow64\GDI32.dll
C:\Windows\syswow64\LPK.dll
C:\Windows\syswow64\USP10.dll
C:\Windows\SysWOW64\MPR.dll
C:\Windows\syswow64\ole32.dll
C:\Windows\syswow64\OLEAUT32.dll
C:\Windows\SysWOW64\Secur32.dll
C:\Windows\syswow64\WS2_32.dll
C:\Windows\syswow64\NSI.dll
C:\Windows\SysWOW64\framedynos.dll
C:\Windows\SysWOW64\WTSAPI32.dll
C:\Windows\SysWOW64\NETAPI32.dll
C:\Windows\SysWOW64\netutils.dll
C:\Windows\SysWOW64\srvcli.dll
C:\Windows\SysWOW64\wkscli.dll
C:\Windows\SysWOW64\dbghelp.dll
C:\Windows\syswow64\SHLWAPI.dll
C:\Windows\SysWOW64\IMM32.DLL
C:\Windows\syswow64\MSCTF.dll
C:\Windows\syswow64\CLBCatQ.DLL
C:\Windows\SysWOW64\wbem\wbemprox.dll
C:\Windows\SysWOW64\wbemcomn.dll
C:\Windows\SysWOW64\Winsta.dll
C:\Windows\SysWOW64\CRYPTSP.dll
C:\Windows\SysWOW64\rsaenh.dll
C:\Windows\SysWOW64\RpcRtRemote.dll
C:\Windows\SysWOW64\wbem\wbemsvc.dll
C:\Windows\SysWOW64\wbem\fastprox.dll
C:\Windows\SysWOW64\NTDSAPI.dll

Files Activity

This sections shows all created or modified files that have been detected during the execution.

Analysis is based on the detection of data blobs which are written on file system. In some cases, multiple blobs could be detected depending how file system operations are performed by the program.

cmd.exe (PID:820)

File activity for process cmd.exe (pid:820)

OPENED ACTION

\SystemRoot\Prefetch\CMD.EXE-AC113AA8.pf
\KnownDlls
C:\Windows **(2 times)**
\KnownDlls32
C:\Users\Administrateur\Downloads\ **(3 times)**
\BaseNamedObjects
C:\
C:\Users\
C:\Users\Administrateur\
c:\ **(2 times)**
c:\Users\Administrateur\Downloads\ **(3 times)**
c:\Users\Administrateur\Downloads\Close_Goose.bat **(6 times)**
c:\Users\Administrateur\Downloads\Close_Goose.bat
c:\Users\Administrateur\Downloads **(3 times)**
c:\Users\Administrateur **(3 times)**
c:\Users\Administrateur\ **(2 times)**
c:\Users **(3 times)**
c:\Users\ **(2 times)**
C:
MountPointManager
\Device\HarddiskVolume2 **(2 times)**
C:\Users\Administrateur\Downloads\taskkill
C:\Windows\SysWOW64\ **(3 times)**
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\SysWOW64\taskkill.exe

QUERY ACTION

C:\Windows\system32\wow64log.dll
C:\Users\Administrateur\Downloads **(3 times)**
c:\Users\Administrateur\Downloads\Close_Goose.bat

taskkill.exe (PID:1268)

File activity for process taskkill.exe (pid:1268)

OPENED ACTION

\SystemRoot\Prefetch\TASKKILL.EXE-E0105477.pf
\KnownDlls
C:\Windows **(2 times)**
\KnownDlls32
C:\Users\Administrateur\Downloads\
C:\Windows\SysWOW64\en-US\taskkill.exe.mui
\Sessions\1\BaseNamedObjects
C:\Windows\syswow64\en-US\KERNELBASE.dll.mui
\Device\KsecDD
C:\Windows\Globalization\Sorting\sortdefault.nls

\Sessions\1\Windows\WindowStations

QUERY ACTION

C:\Windows\system32\wow64log.dll
C:\Windows\SysWOW64\rpcss.dll (2 times)
C:\Windows\SysWOW64\wbem\wbemcomn.dll
C:\Windows\SysWOW64\wbem\Logs\
C:\Windows\SysWOW64\taskkill.exe **(2 times)**
C:\Windows\SysWOW64\wbem\NTDSAPI.dll

Processes details

This sections shows detail on processes that have been detected during the execution.

For each process, "creation mode" possible values are:

- *New: Occured when a new process is detected.*
- *Injected: Occured when injection code is dectected.*
- *Rpc: Occured when a new process is created by the task scheduler or the service management*

cmd.exe (PID: 820)

Process name	cmd.exe
Process ID	820
Creation mode	
Path	C:\Windows\syswow64\cmd.exe
Command line	C:\Windows\syswow64\cmd.exe /C c:\Users\Administrateur\Downloads\Close_Goose.bat

taskkill.exe (PID: 1268)

Process name	taskkill.exe
Process ID	1268
Creation mode	
Path	C:\Windows\SysWOW64\taskkill.exe
Command line	taskkill /f /im goosedesktop.exe
Parent PID	820

Registry Activity

This sections shows activity on Windows registry by listing created or modified registry keys.

cmd.exe (PID: 820)

Registry activity for process cmd.exe (PID: 820)

READ ACTION

\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS

Value
DisableUserModeCallbackFilter
DisableUserModeCallbackFilter
DisableLocalOverride

\Registry\Machine\System\CurrentControlSet\Control\Session Manager

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER

Value
CWDIllegalInDLLSearch
CWDIllegalInDLLSearch
SafeDllSearchMode

\Registry\Machine\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

Value

\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option

Value

\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers

Value

\REGISTRY\MACHINE\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\SAFER\CODEIDENTIFIERS

Value
TransparentEnabled
Levels
DefaultLevel
SaferFlags
PolicyScope
LogFileName
TransparentEnabled
AuthenticodeEnabled

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers

Value

\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS

Value
(Default)

\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager

Value

\REGISTRY\MACHINE

Value

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Diagnostics

Value

\Registry\Machine\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\GRE_Initialize

Value

\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\GRE_INITIALIZE

Value
DisableMetaFiles

\Registry\Machine\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Compatibility32

Value

\REGISTRY\MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\COMPATIBILITY32

Value
cmd

\Registry\Machine\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\IME Compatibility

Value

\Registry\MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CustomLocale

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE

Value
EMPTY
EMPTY
en-US

\Registry\Machine\System\CurrentControlSet\Control\NLS\Language

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LANGUAGE

Value
InstallLanguageFallback

\Registry\Machine\System\CurrentControlSet\Control\MUI\UILanguages

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\MUI\UILANGUAGES

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\MUI\UILANGUAGES\en-US

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\MUI\UILANGUAGES\EN-US

Value
Type
AlternateCodePage

\Registry\Machine\System\CurrentControlSet\Control\MUI\UILanguages\PendingDelete

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\MUI\Settings

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Control Panel\Desktop\MuiCached\MachineLanguageConfiguration

Value

\Registry\Machine\System\CurrentControlSet\Control\MUI\Settings\LanguageConfiguration

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\MUI\SETTINGS\LANGUAGECONFIGURATION

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Control Panel\Desktop

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Control Panel\Desktop\LanguageConfiguration

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\CONTROL PANEL\DESKTOP\LANGUAGECONFIGURATION

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Control Panel\Desktop

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\CONTROL PANEL\DESKTOP

Value
PreferredUILanguages

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Control Panel\Desktop\MuiCached

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\CONTROL PANEL\DESKTOP\MUICACHED

Value
MachinePreferredUILanguages
MachinePreferredUILanguages

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows

Value

\REGISTRY\MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWS

Value
LoadAppInit_DLLs

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\System

Value

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Command Processor

Value

\REGISTRY\MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\COMMAND PROCESSOR

Value
DisableUNCCheck
EnableExtensions
DelayedExpansion
DefaultColor
CompletionChar
PathCompletionChar
AutoRun

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Microsoft\Command Processor

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\SOFTWARE\MICROSOFT\COMMAND PROCESSOR

Value
DisableUNCCheck
EnableExtensions
DelayedExpansion
DefaultColor
CompletionChar
PathCompletionChar
AutoRun

\Registry\Machine\System\CurrentControlSet\Control\Nls\CustomLocale

Value

\Registry\Machine\System\CurrentControlSet\Control\Nls\ExtendedLocale

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\EXTENDEDLOCALE

Value
en-US

\Registry\Machine\System\CurrentControlSet\Control\Nls\Locale

Value

\Registry\Machine\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts

Value

\Registry\Machine\System\CurrentControlSet\Control\Nls\Language Groups

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LOCALE

Value
00000409

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LANGUAGE GROUPS

Value
1

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\LevelObjects

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Paths

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hashes

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\UrlZones

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\4096\Paths

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\4096\Hashes

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\4096\UrlZones

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\65536\Paths

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\65536\Hashes

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\65536\UrlZones

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\131072\Paths

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\131072\Hashes

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\131072\UrlZones

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Paths

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\Hashes

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144\UrlZones

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Path

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\Hash

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\0\UrlZo

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\4096\P

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\4096\H

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\4096\U

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\65536

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\65536

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\65536

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\131072

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\131072

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\131072

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers\262144

Value

\Registry\Machine\System\CurrentControlSet\Control\Srp\\GP

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\SRP\GP

Value
RuleCount

\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager\AppCertDlls

Value

\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager\AppCompatibility

Value

\Registry\MACHINE\Software\Wow6432Node\Policies\Microsoft\Windows\AppCompat

Value

\REGISTRY\MACHINE\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\APPCOMPAT

Value
(Default)

\Registry\MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide

Value

\REGISTRY\MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\SIDEBYSIDE

Value
PreferExternalManifest

taskkill.exe (PID: 1268)

Registry activity for process taskkill.exe (PID: 1268)

READ ACTION

\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\IMAGE FILE EXECUTION OPTIONS

Value
DisableUserModeCallbackFilter
DisableUserModeCallbackFilter

\Registry\Machine\System\CurrentControlSet\Control\Session Manager

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\SESSION MANAGER

Value
CWDIllegalInDLLSearch
CWDIllegalInDLLSearch
SafeDllSearchMode
SafeProcessSearchMode

\Registry\Machine\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options

Value

\Registry\MACHINE\System\CurrentControlSet\Control\SafeBoot\Option

Value

\Registry\Machine\System\CurrentControlSet\Control\Srp\GP\DLL

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\Windows\Safer\CodeIdentifiers

Value

\REGISTRY\MACHINE\SOFTWARE\POLICIES\MICROSOFT\WINDOWS\SAFER\CODEIDENTIFIERS

Value
TransparentEnabled

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers

Value

\Registry\Machine\System\CurrentControlSet\Control\Nls\Sorting\Versions

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\SORTING\VERSIONS

Value
(Default)

\REGISTRY\MACHINE

Value

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Diagnostics

Value

\Registry\MACHINE\System\CurrentControlSet\Control\Session Manager

Value

\Registry\Machine\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\GRE_Initialize

Value

\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENTVERSION\GRE_INITIALIZE

Value
DisableMetaFiles

\Registry\Machine\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Compatibility32

Value

\REGISTRY\MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\COMPATIBILITY32

Value
taskkill

\Registry\Machine\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\IME Compatibility

Value

\Registry\MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CustomLocale

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\CUSTOMLOCALE

Value
EMPTY
EMPTY
en-US
en

\Registry\Machine\System\CurrentControlSet\Control\NLS\Language

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\LANGUAGE

Value
InstallLanguageFallback

\Registry\Machine\System\CurrentControlSet\Control\MUI\UILanguages

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\MUI\UILANGUAGES

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\MUI\UILANGUAGES\en-US

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\MUI\UILANGUAGES\EN-US

Value
Type
AlternateCodePage

\Registry\Machine\System\CurrentControlSet\Control\MUI\UILanguages\PendingDelete

Value

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\MUI\Settings

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Control Panel\Desktop\MuiCached\MachineLanguageConfiguration

Value

\Registry\Machine\System\CurrentControlSet\Control\MUI\Settings\LanguageConfiguration

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\MUI\SETTINGS\LANGUAGECONFIGURATION

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Software\Policies\Microsoft\Control Panel\Desktop

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Control Panel\Desktop\LanguageConfiguration

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\CONTROL PANEL\DESKTOP\LANGUAGECONFIGURATION

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Control Panel\Desktop

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\CONTROL PANEL\DESKTOP

Value
PreferredUILanguages

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\Control Panel\Desktop\MuiCached

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003\CONTROL PANEL\DESKTOP\MUICACHED

Value
MachinePreferredUILanguages
MachinePreferredUILanguages

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows

Value

\REGISTRY\MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS NT\CURRENTVERSION\WINDOWS

Value
LoadAppInit_DLLs

\REGISTRY\MACHINE\system\CurrentControlSet\control\NetworkProvider\HwOrder

Value

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\OLE

Value

\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\OLE

Value
PageAllocatorUseSystemHeap
PageAllocatorSystemHeapIsPrivate
MaxSxSHashCount
MaximumAllowedAllocationSize

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\OLE\Tracing

Value

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\OLEAUT

Value

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\WBEM\CIMOM

Value

\REGISTRY\MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WBEM\CIMOM

Value
Logging
Logging
Logging Directory
Logging Directory
Logging
Log File Max Size
ProcessID
EnablePrivateObjectHeap
ContextLimit
ObjectLimit
IdentifierLimit
EnableObjectValidation

\REGISTRY\MACHINE\System\CurrentControlSet\Services\LanmanWorkstation\Parameters

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\SERVICES\LANMANWORKSTATION\PARAMETERS

Value
RpcCacheTimeout

\Registry\Machine\Software\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR

Value

\REGISTRY\MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\WINDOWS ERROR REPORTING\WMR

Value
Disable

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Rpc

Value

\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\RPC

Value
MaxRpcSize

\Registry\Machine\System\CurrentControlSet\Control\ComputerName\ActiveComputerName

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACTIVECOMPUTERNAME

Value
ComputerName
ComputerName

\Registry\Machine\System\Setup

Value

\REGISTRY\MACHINE\SYSTEM\SETUP

Value
OOBEInProgress
SystemSetupInProgress
OOBEInProgress
SystemSetupInProgress

\REGISTRY\MACHINE\Software\Wow6432Node\Policies\Microsoft\Windows NT\Rpc

Value

\Registry\Machine\Software\Policies\Microsoft\SQMClient\Windows

Value

\Registry\Machine\Software\Microsoft\SQMClient\Windows

Value

\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\SQMCLIENT\WINDOWS

Value
CEIPEnable

\Registry\User\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\AppID\taskkill.exe

Value

\Registry\Machine\Software\Classes\AppID\taskkill.exe

Value

\Registry\Machine\System\CurrentControlSet\Control\Lsa

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\LSA

Value
EveryoneIncludesAnonymous
FipsAlgorithmPolicy

\REGISTRY\MACHINE\Software\Microsoft\COM3

Value

\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\COM3

Value
Com+Enabled

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\CLSID\{4590F811-1D3A-11D0-891F-00AA

Value

\Registry\Machine\Software\Classes\Wow6432Node\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}

Value
(Default)
(Default)

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{4590F811-1D3A-11D0-891F-00AA0

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\TreatAs

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{4590F811-1D3A-11D0-891F-00AA0

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}

Value

\Registry\Machine\Software\Classes\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\Prog

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{4590F811-1D3A-11D0-891F-00AA0

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{4590F811-1D3A-11D0-891F-00AA0

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocServer32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\INPROCSERVER32

Value
InprocServer32
(Default)
(Default)
(Default)
ThreadingModel

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{4590F811-1D3A-11D0-891F-00AA0

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocHandler32

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{4590F811-1D3A-11D0-891F-00AA0

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F811-1D3A-11D0-891F-00AA004B2E24}\InprocHandler

Value

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\OLE

Value

\Registry\Machine\System\CurrentControlSet\Control\Nls\CustomLocale

Value

\Registry\Machine\System\CurrentControlSet\Control\Nls\ExtendedLocale

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\NLS\EXTENDEDLOCALE

Value
en-US
en

\Registry\Machine\System\CurrentControlSet\Services\Tcpip\Parameters

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\SERVICES\TCPIP\PARAMETERS

Value
Hostname
Domain
Hostname
Domain

\Registry\Machine\Software\Wow6432Node\Policies\Microsoft\System\DNSclient

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}

Value

\Registry\Machine\Software\Classes\Wow6432Node\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}

Value
(Default)
(Default)

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\TreatAs

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\TreatAs

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\Progid

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}

Value

\Registry\Machine\Software\Classes\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\Progid

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\InprocServer32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\InprocServer32

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\InprocHandler32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\InprocHandler32

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\InprocHandler

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{8BC3F05E-D86B-11D0-A075-00C04FB68820}\InprocHandler

Value

\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Defaults\Provider\Microsoft Strong Cryptographic Provider

Value

\REGISTRY\MACHINE\SOFTWARE\WOW6432NODE\MICROSOFT\CRYPTOGRAPHY\DEFAULTS\PROVIDER\MICROSOFT STRONG CRYPTOGRAPHIC PROVIDER

Value
Type
Image Path
Image Path
Image Path
Image Path

\Registry\Machine\System\CurrentControlSet\Control\Lsa\FipsAlgorithmPolicy

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\LSA\FIPSALGORITHMPOLICY

Value
Enabled

\Registry\Machine\SYSTEM\CurrentControlSet\Policies\Microsoft\Cryptography\Configuration

Value

\REGISTRY\MACHINE\Software\Policies\Microsoft\Cryptography

Value

\REGISTRY\MACHINE\SOFTWARE\POLICIES\MICROSOFT\CRYPTOGRAPHY

Value
PrivKeyCacheMaxItems
PrivKeyCachePurgeIntervalSeconds
PrivateKeyLifetimeSeconds

\REGISTRY\MACHINE\Software\Microsoft\Cryptography

Value

\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\CRYPTOGRAPHY

Value
MachineGuid
MachineGuid
MachineGuid
MachineGuid

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Offload

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\Interface\{00000134-0000-0000-C000-000000000046}

Value

\Registry\Machine\Software\Classes\Wow6432Node\Interface\{00000134-0000-0000-C000-000000000046}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{00000134-0000-0000-C000-000000000046}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\Interface\{00000134-0000-0000-C000-000000000046}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{00000134-0000-0000-C000-000000000046}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{00000134-0000-0000-C000-000000000046}\PROXYSTUBCLSID32

Value
(Default)

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Rpc\Extensions

Value

\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\RPC\EXTENSIONS

Value
NdrOleExtDLL
RemoteRpcDll

\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\BFE

Value

\Registry\Machine\Software\Microsoft\SQMClient\Windows\DisabledProcesses

Value

\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\SQMCLIENT\WINDOWS\DISABLEDPROCESSES

Value
243A6011

\Registry\Machine\Software\Microsoft\SQMClient\Windows\DisabledSessions

Value

\REGISTRY\MACHINE\SOFTWARE\MICROSOFT\SQMCLIENT\WINDOWS\DISABLEDSESSIONS

Value
MachineThrottling
GlobalSession

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\Ole

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\Interface\{F309AD18-D86A-11D0-A075-00C04FB68820}

Value

\Registry\Machine\Software\Classes\Wow6432Node\Interface\{F309AD18-D86A-11D0-A075-00C04FB68820}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{F309AD18-D86A-11D0-A075-00C04FB68820}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\Interface\{F309AD18-D86A-11D0-A075-00C04FB68820}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{F309AD18-D86A-11D0-A075-00C04FB68820}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{F309AD18-D86A-11D0-A075-00C04FB68820}\PROXYSTUBCLSID32

Value
(Default)

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\CLSID\{7C857801-7381-11CF-884D-00AA

Value

\Registry\Machine\Software\Classes\Wow6432Node\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}

Value
(Default)
(Default)

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{7C857801-7381-11CF-884D-00AA0

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\TreatAs

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{7C857801-7381-11CF-884D-00AA0

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}

Value

\Registry\Machine\Software\Classes\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\Progi

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{7C857801-7381-11CF-884D-00AA0

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{7C857801-7381-11CF-884D-00AA0

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\InprocServer32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\INPROCSERVER32

Value
InprocServer32
(Default)
(Default)
(Default)
ThreadingModel

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{7C857801-7381-11CF-884D-00AA0

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{7C857801-7381-11CF-884D-00AA0

Value

\REG-ISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\InprocHandler32

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{7C857801-7381-11CF-884D-00AA0

Value

\REG-ISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{7C857801-7381-11CF-884D-00AA004B2E24}\InprocHandler

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}

Value

\Registry\Machine\Software\Classes\Wow6432Node\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\Interface\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{D4781CD6-E5D3-44DF-AD94-930EFE48A887}\PROXYSTUBCLSID32

Value
(Default)

\Registry\Machine\System\CurrentControlSet\Control\ComputerName

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME

Value

\REGISTRY\MACHINE\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ActiveComputerName

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}

Value

\Registry\Machine\Software\Classes\Wow6432Node\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}

Value
(Default)
(Default)

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\TreatAs

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\TreatAs

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\Progid

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}

Value

\Registry\Machine\Software\Classes\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\Progid

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\InprocServer32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\InprocServer32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\INPROCSERVER32

Value
InprocServer32
(Default)
(Default)
(Default)
ThreadingModel

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\InprocHandler32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\InprocHandler32

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\InprocHandler

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{674B6698-EE92-11D0-AD71-00C04FD8FDFF}\InprocHandler

Value

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\WBEM\CIMOM

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}

Value

\Registry\Machine\Software\Classes\Wow6432Node\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{9556DC99-828C-11CF-A37E-00AA003240C7}

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\Interface\{9556DC99-828C-11CF-A37E-00AA003240C7}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{9556DC99-828C-11CF-A37E-00AA003240C7}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{9556DC99-828C-11CF-A37E-00AA003240C7}\PROXYSTUBCLSID32

Value
(Default)

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}

Value

\Registry\Machine\Software\Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}

Value
(Default)
(Default)

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\TreatAs

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\TreatAs

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\Progid

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}

Value

\Registry\Machine\Software\Classes\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\Progid

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocServer32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\INPROCSERVER32

Value
InprocServer32
(Default)
(Default)
(Default)
ThreadingModel

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocHandler32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocHandler32

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocHandler

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{D68AF00A-29CB-43FA-8504-CE99A996D9EA}\InprocHandler

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\Interface\{027947E1-D731-11CE-A357-000000000001}

Value

\Registry\Machine\Software\Classes\Wow6432Node\Interface\{027947E1-D731-11CE-A357-000000000001}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{027947E1-D731-11CE-A357-000000000001}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\Interface\{027947E1-D731-11CE-A357-000000000001}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{027947E1-D731-11CE-A357-000000000001}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{027947E1-D731-11CE-A357-000000000001}\PROXYSTUBCLSID32

Value
(Default)

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}

Value

\Registry\Machine\Software\Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}

Value
(Default)
(Default)

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\TreatAs

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\TreatAs

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\Progid

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}

Value

\Registry\Machine\Software\Classes\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\Progid

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\Progid

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocServer32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\INPROCSERVER32

Value
InprocServer32
(Default)
(Default)
(Default)
ThreadingModel

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocHandler32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocHandler32

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocHandler

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{1B1CAD8C-2DAB-11D2-B604-00104B703EFD}\InprocHandler

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}

Value

\Registry\Machine\Software\Classes\Wow6432Node\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{1C1C45EE-4395-11D2-B60B-00104B703EFD}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\Interface\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{1C1C45EE-4395-11D2-B60B-00104B703EFD}\PROXYSTUBCLSID32

Value
(Default)

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}

Value

\Registry\Machine\Software\Classes\Wow6432Node\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{423EC01E-2E35-11D2-B604-00104B703EFD}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\Interface\{423EC01E-2E35-11D2-B604-00104B703EFD}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{423EC01E-2E35-11D2-B604-00104B703EFD}\ProxyStubClsid32

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\INTERFACE\{423EC01E-2E35-11D2-B604-00104B703EFD}\PROXYSTUBCLSID32

Value
(Default)

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\Wow6432Node\CLSID\{4590F812-1D3A-11D0-891F-00AA

Value

\Registry\Machine\Software\Classes\Wow6432Node\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}

Value
(Default)
(Default)

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{4590F812-1D3A-11D0-891F-00AA0

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}\TreatAs

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{4590F812-1D3A-11D0-891F-00AA0

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_CLASSES\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}

Value

\Registry\Machine\Software\Classes\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}\Prog

Value

\REGISTRY\MACHINE\SOFTWARE\CLASSES\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}\Progid

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{4590F812-1D3A-11D0-891F-00AA0

Value

\REGISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{4590F812-1D3A-11D0-891F-00AA0

Value

\REG-ISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}\InprocServer32

Value

\REG-ISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}\INPROCSERVER32

Value
InprocServer32
(Default)
(Default)
(Default)
ThreadingModel

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{4590F812-1D3A-11D0-891F-00AA0

Value

\REG-ISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}\InprocHandler32

Value

\REG-ISTRY\USER\S-1-5-21-2347412131-2503537479-2540737720-1003_Classes\Wow6432Node\CLSID\{4590F812-1D3A-11D0-891F-00AA0

Value

\REG-ISTRY\MACHINE\SOFTWARE\CLASSES\WOW6432NODE\CLSID\{4590F812-1D3A-11D0-891F-00AA004B2E24}\InprocHandler

Value

CREATE ACTION

\REGISTRY\MACHINE\Software\Wow6432Node\Microsoft\WBEM\CIMOM

Sleeps Activity

Sleeps are sometimes used by programs for synchronization, but can also be used to evade from analysis.

taskkill.exe (PID: 1268)

Sleeps activity for process taskkill.exe (PID: 1268)

Duration (ms)	Occurrences
60000	5

CPUID Activity

CPUID are instructions used by software to request information about CPU.

cmd.exe (PID: 820)

CPUID activity for process cmd.exe (PID: 820)

Leaf parameter (hex)	Subleaf parameter (hex)	Occurrences
0x0	0x246	**1**
0x1	0x6c65746e	**1**

taskkill.exe (PID: 1268)

CPUID activity for process taskkill.exe (PID: 1268)

Leaf parameter (hex)	Subleaf parameter (hex)	Occurrences
0x0	0x246	**2**
0x1	0x6c65746e	**2**
0x1	0x0	**2**
0x0	0x0	**2**
0x0	0x22e1a8	**1**
0x1	0x1	**1**

Window Activity

taskkill.exe (PID: 1268)

FIND WINDOW

Window class	Window name	Occurrences
		94

End of document