Malware Analysis Appliance by Blue Coat Systems, Inc.

Task Details

Host: mag2, Sample ID: 621, Task ID: 2431

Task ID: 2431 Risk Level: 5

Date Processed: 2016-02-22 05:29:33 (UTC)

Processing Time: 62.01 seconds
Virtual Environment: IntelliVM

Execution Arguments:

c:\windows\temp\677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5.exe"

Sample ID: 621
Type: basic
Owner: admin

Label: 677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5

Date Added: 2016-02-22 05:26:49 (UTC)

File Type: PE32:win32:gui File Size: 506409 bytes

MD5: 2d9511520df41b9010d25193b67ac416

SHA256: 677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5

Description: None

Pattern Matching Results

4 Reads process memory

- 5 Abnormal sleep detected
- 4 Register or unregister a DLL from command line
- 2 PE: Nonstandard section
- 3 Long sleep detected
- 4 Checks whether debugger is present
- 5 PE: Contains compressed section

Static Events

Anomaly: PE: Contains one or more non-standard sections

Process/Thread Events

Creates process:

C:\windows\temp\677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5.exe ["C:\windows\temp\677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5.exe"]

Creates process: C:\Windows\system32\regsvr32.exe [regsvr32.exe]
Reads from process: PID:2512 C:\Windows\System32\regsvr32.exe
Writes to process: PID:2512 C:\Windows\System32\regsvr32.exe

Terminates process:

 $C: \verb|Windows| Temp| 677926883 abd 5e9e34c0 ac 6435a9272a3 be 5efc9ab7e97c5e01b12b6e5d75fb5.exe for the control of the contro$

Named Object Events

Creates mutex: \Sessions\1\BaseNamedObjects\DBWinMutex

Creates event: \Sessions\1\BaseNamedObjects\38FB558AE1FDC9D1C1ABCBEB8FE66A0A

Creates event: \KernelObjects\MaximumCommitCondition

File System Events

Opens: C:\Windows\Prefetch\677926883ABD5E9E34C0AC6435A92-0B89DE20.pf

Opens: C:\Windows\System32

Opens:

C:\windows\temp\677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5.exe.Local

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-

controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af

Opens: C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_5.82.7601.17514_none_ec83dffa859149af\comctl32.dll

Opens: C:\Windows\System32\sechost.dll
Opens: C:\windows\temp\VERSION.dll
Opens: C:\Windows\System32\version.dll
Opens: C:\Windows\System32\imm32.dll
Opens: C:\Windows\System32\uxtheme.dll

Opens: C:\Windows\Globalization\Sorting\SortDefault.nls

Opens: C:\windows\temp\dwmapi.dll
Opens: C:\Windows\System32\dwmapi.dll

Opens: C:\Users\Admin\Desktop

Opens: C:\windows\temp\é† éŽ'é-"éž-é¦~鮚鶜龞ê† êŽ¢ê-¤êž¦ê¦¨ê®ªê¶¬ê¾®ë†°ë޲ë-´ëž¶ë¦¸ë®°ë¶¼ë¾¾ì‡€ì ,ì—"쟆ì§^쯊ì∙Œì¿Ží‡ í 'í-"íŸ-í§~ô†§œí¿žî‡ î ¢î-¤îŸ¦î§~ï ²ï-

´ïŸ¶ïŚ,ï″ĸĭ¿¾ï°″ 濫 Ä Ì,Ô"Ütà¤^ଊā′Œà¼Žá" áŒ'á″″áœ-á¤^ᬚá′œá¼žâ" ጢâ″¤âœ¦â¤ï⬰â ´¬â¼®ã"°ãŒ²ã″′㜶⤏㬰ã′¼ã¼¾ä…€ä 'ä•"ä tä¥^ãŠäµŒä½Žå… å 'å•″å –å¥~ãšåµœå½žä… ä 'ä•"ä tä¥^ä-

ŠäμŒä½Žå… å 'å•"å -å¥~çšçμ¼ç½¾èt€èŽ,è-"èžtè¦^變趌辎ét éŽ'é-"éž-é¦~鮊鶌龎êt êŽcê-¤êž¦ê¦~ꮪê¶-ê¾®ët°ë޲‰

Opens: $C:\acute{e}t$ $\acute{e}\check{Z}'\acute{e}-"\acute{e}\check{z}-\acute{e}|^{\sim}\acute{e}\mathscr{B}\check{s}^{-}\mathscr{C}=-\check{e}\check{Z}+\check{e}|^{\sim}\acute{e}\mathscr{B}^{-}\acute{e}^{-}\mathscr{C}=-\check{e}\check{Z}+\check{e}|^{\sim}\acute{e}\mathscr{B}^{-}\acute{e}^{-}\mathscr{C}=-\check{e}\check{Z}+\check{e}|^{\sim}\acute{e}\mathscr{B}^{-}\acute{e}^{-}\mathscr{C}=-\check{e}\check{Z}+\check{e}|^{\sim}\acute{e}\mathscr{B}^{-}\acute{e}^{-}$

´ëž¶ë¦¸ë®°ë¶¼ë¾¾i‡€ì ,ì—"쟆ì§^쯊췌쿎í‡ í 'í—"íŸ−í§~ô†§œí¿žî‡ î ¢î—¤îŸ¦î§¨î¯°î·¬î¿®ï‡°ï ²ï— ´ïŸ¶ï§¸ï¯°ï·¼ï;¾ï°¨ 濫 Ä Ì,Ô"܆à¤^ଊà′Œà¼Žá" ጒá""áœ-á¤~ᬚá′œá¼žâ" ⌢â"¤âœ¦â¤¨â¬ªâ

´¬â¼®ã"°ãŒ²ã″´ãœ¶ã¤¸ã¬°ã′¼ã¼¾ä…€ä ,ä•"ä tä¥^äŠäµŒä½Žå… å 'å•″å –å¥~åšåµœå½žä… ä ,ä•"ä tä¥^ä-

```
ŠäμŒä½Žå… å 'å•"å -å¥~çšçμ¼ç½¾èt€èŽ,è-"螆è¦^變趌辎é† éŽ'é-"éž-é¦~鮊鶌龎ê† êŽ¢ê-
¤êž¦ê¦"ꮪ궬꾮놰뎲‰
                                                                                                        C:\Windows\system32\\equiv \( \equiv \) \\equiv \( \equiv \) \\\equiv \\equiv \) \\\equiv \( \equiv \) \\\equiv \( \equiv \) \\\equiv \\equiv \) \\\equiv \( \equiv \) \\\equiv \\equiv \) \\\equiv \\equiv \) \\\equiv \( \equiv \) \\\equiv \\equiv \\equiv \\equiv \) \\\equiv \\equiv \
      Opens:
¤êž¦ê¦¨ê®ªê¶¬ê¾®ë†°ë޲ë-´ëž¶ë¦຺뮰붼达쇀ì ,ì—"쟆ì§^쯊췌쿎í‡ í ′í—″íŸ-í§~ô†§œí¿žî‡ î ¢î—
 \label{eq:control_problem} \text{$\tt u$} \ddot{\Gamma}^{\dagger} \dot{\Gamma}^{\bullet} \ddot{\Gamma}^{\bullet} 
´œá¼žâ" ⌢â″¤âœ¦â¤¨â¬ªâ′¬â¼®ã"°ãŒ²ã″′㜶㤸㬰ã′¼ã¼¾ä…€ä 'ä•"ä tä¥^ãŠäμŒã½Žå… å 'å•″å –å¥´å-
šåμœå½žä… ä ,ä•"ä tä¥^äŠäμŒä½Žå… å ′å•″å -å¥~çšçμ¼ç½¾èt€èŽ,è-"èžtè¦^變趌辎ét éŽ′é-″éž-
\label{eq:continuity} \'e'_-\'e@Š\'e^\P \ree^3/\'E^\dagger - \'e^2/\'e^- = \ree^2/\'e^- = \ree^3/\ree^3/\ree^3/\ree^3/\ree^3/\ree^3/\ree^3/\ree^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee^3/\reee
                                                                                                       C:\Windows\system\é† éŽ'é-"éž-é¦~鮚鶜龞ê† êŽ¢ê-
      Opens:
¤êž¦ê¦¨ê®ªê¶¬ê¾®ë†°ë޲ë-´ëž¶ë¦¸ë®°ë¶¼ë¾¾ì‡€ì ,ì-"쟆ì§^췌쿎í‡ í 'í-″íŸ-í§~ô†§œí¿žî‡ î ¢î-
 \ddot{\text{u}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}}\ddot{\text{U}
´œá¼žâ" ⌢â″¤âœ¦â¤¨â¬ªâ′¬â¼®ã"°ãŒ²ã″′㜶㤸㬰ã′¼ã¼¾ä…€ä 'ä•"ä tä¥^ãŠäμŒã½Žå… å 'å•″å –å¥´å-
šåμœå½žä… ä ,ä•"ä tä¥^äŠäμŒä½Žå… å ′å•″å -å¥~çšçμ¼ç½¾èt€èŽ,è-"èžtè¦^變趌辎ét éŽ′é-″éž-
C:\Windows\ét éŽ'é-"éž-é¦~鮚鶜龞êt ꎢê-¤êž¦ê¦¨ê®ªê¶¬ê¾®ët°ë޲ë-
      Opens:
 ´ëž¶ë¦、뮰붼뾾1≠€ì ,ì—"쟆ì§^쯊췌쿎í‡ í ′í—″íŸ−í§~ô†§œí¿žî‡ î ¢î—¤îŸ¦î§¨î¯ªî·¬î¿®ï‡°ï ²ï—
´ĭŸ¶īŚĺi∵¼ï¿¾ï°¨ 濫 Ä Ì,Ô"Ütà¤^ଊà′Œà¼Žá" áŒ'á″″᜖á¤~ᬚá′œá¼žâ" ⌢â″¤âœ¦â¤¨â¬ãâ
ʻ¬â¼®ã"°ãŒ²ã″′㜶㤸㬰ã′¼ã¼¾ä…€ä ,ä∙"ä tä¥'äŠäμŒä½Žå… å 'å•″å –å¥'åšåμœå½žä… ä 'ä•"ä tä¥'ä-
ŠäμŒä½Žå… å ′å•″å -å¥~çšςμ¼ς½%èt€èŽ,è-"èžtè¦^變趌辎ét éŽ′é-″éž-é¦~鮊鶌龎êt ꎢê-
¤êž¦ê¦"ꮪ궬꾮놰뎲‰
                                                                                                       C:\Windows\System32\Wbem\é† éŽ'é-"éž-é¦~鮚鶜龞ê† êŽ¢ê-
      Opens:
¤êž¦ê¦¨ê®ªê¶¬ê¾®ët°ë޲ë-´ëž¶ë¦¸ë®°ë¶¼ê¾¾ì‡€ì ,ì-"ìŸtì§^쯊췌쿎í‡ í 'í-″íŸ-í§~ô†§œí¿žî‡ î ¢î-
´œá¼žâ" ⌢â″¤âœ¦â¤¨â¬ªâ´¬â¼®ã"°ãŒ²ã″´ãœ¶ã¤、㬰ã′¼ã¼¾ã…€ä ,ä•"ä †ä¥`ãŠäμŒä½Žå… å ′å•″å –å¥~å-
šåμœå½žä… ä 'ä•"ä tä¥^äŠäμŒä½Žå… å 'å•"å -å¥~çšçμ¼ç½¾èt€èŽ'è-"èžtè¦^變趌辎ét 鎒é-"éž-
Opens:
                                                                                                        C:\Windows\System32\WindowsPowerShell\v1.0\é† éŽ'é-"éž-
馯鮚鶜齞ê† êŽcꗤꎦꦨꮳ궗꾮놰뎲ë–′랶릸ë®°ë¶%ë¾%1‡€ì ,ì—"쟆ì§^쯊i·Œì¿Ží‡ í ′í—″ퟖ
í§~ô†§œí¿žî‡ î ¢î—¤îŸ¦î§~î<sup>~</sup>aï ²ï—′笠ﯰï·%￾ï°¨ 濫 Ä Ì,Ô"Ütà¤^à–Šà
 ´Œà¼Žá" áŒ′á""áœ−á¤~ᬚᴜ἞â" ⌢â"¤âœ¦â¤¨â¬ªâ´¬â¼®ã"°ãŒ²ã"´ãœ¶ã¤¸ã¬°ã´¼ã¼¾ä…€ä 'ä•"ä tä¥^ä-
ŠäμŒä½Žå… å 'å•"å –å¥~åšåμœå½žä… ä 'ä•"ä †ä¥^äŠäμŒä½Žå… å 'å•"å –å¥~çšçμ¼ç½¾è†€èŽ'è–
"èžtè¦^變趌辎ét 鎒é-"éž-é¦~鮊鶌龎êt ꎢê-¤êž¦ê¦¨ê®ªê¶¬ê¾®ët°ëʲ‰
                                                                                                       C:\Windows\System32\C_1256.NLS
      Opens:
      Opens:
                                                                                                        C:\Windows\System32\C_1251.NLS
                                                                                                        C:\Windows\System32\C_950.NLS
      Opens:
      Opens:
                                                                                                        C:\Windows\System32\C_1250.NLS
      Opens:
                                                                                                        C:\Windows\System32\C_1253.NLS
                                                                                                        C:\Windows\System32\C_1255.NLS
      Opens:
      Opens:
                                                                                                        C:\Windows\System32\C_932.NLS
      Opens:
                                                                                                        C:\Windows\System32\C_949.NLS
                                                                                                        C:\Windows\System32\C_874.NLS
      Opens:
      Opens:
                                                                                                        C:\Windows\System32\C_1254.NLS
                                                                                                       C:\Windows\System32\C_1257.NLS
C:\Windows\System32\C_1258.NLS
      Opens:
      Opens:
      Opens:
                                                                                                        C:\Windows\System32\C_936.NLS
      Opens:
                                                                                                        C:\windows\temp\wsock32.dll
                                                                                                       C:\Windows\System32\wsock32.dll
      Opens:
      Opens:
                                                                                                        C:\windows\temp\winmm.dll
                                                                                                       C:\Windows\System32\winmm.dll
      Opens:
      Opens:
                                                                                                        C:\windows\temp\atl.dll
      Opens:
                                                                                                        C:\Windows\System32\atl.dll
      Opens:
                                                                                                        C:\windows\temp\wtsapi32.dll
      Opens:
                                                                                                        C:\Windows\System32\wtsapi32.dll
      Opens:
C:\windows\temp\677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5.ENU
      Opens:
C:\windows\temp\677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5.ENU.DLL
      Opens:
C:\windows\temp\677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5.EN
C:\windows\temp\677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5.EN.DLL
      Opens:
                                                                                                       C:\Windows
      Opens:
                                                                                                        C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
      Opens:
                                                                                                        C:\Windows\System32\mshta.exe
                                                                                                        C:\Windows\System32\rpcss.dll
      Opens:
      Opens:
                                                                                                        C:\windows\temp\CRYPTBASE.dll
      Opens:
                                                                                                        C:\Windows\System32\cryptbase.dll
                                                                                                        C:\Windows\System32\wbem\wbemprox.dll
      Opens:
      Opens:
                                                                                                        C:\Windows\system32\wbem\wbemcomn.dll
      Opens:
                                                                                                        C:\Windows\System32\wbemcomn.dll
                                                                                                        C: \verb|\windows\System32\wbem\Logs||
      Opens:
      Opens:
                                                                                                        C:\windows\temp\CRYPTSP.dll
      Opens:
                                                                                                        C:\Windows\System32\cryptsp.dll
      Opens:
                                                                                                        C:\Windows\System32\rsaenh.dll
      Opens:
                                                                                                        C:\windows\temp\RpcRtRemote.dll
                                                                                                        C:\Windows\System32\RpcRtRemote.dll
      Opens:
      Opens:
                                                                                                        C:\Windows\System32\wbem\wbemsvc.dll
                                                                                                        C:\Windows\System32\wbem\fastprox.dll
      Opens:
      Opens:
                                                                                                        C:\Windows\system32\wbem\NTDSAPI.dll
      Opens:
                                                                                                        C:\Windows\System32\ntdsapi.dll
      Opens:
                                                                                                        C:\windows\temp\regsvr32.exe
                                                                                                        C:\Windows\System32\regsvr32.exe
      Opens:
```

C:\Windows\System32\apphelp.dll

Opens:

Opens: C:\Windows\AppPatch\sysmain.sdb

Opens: C:\Windows\Prefetch\REGSVR32.EXE-8461DBEE.pf

Opens: C:

Opens: C:\\$Extend
Opens: C:\ProgramData

Opens: C:\ProgramData\Microsoft
Opens: C:\ProgramData\Microsoft\Windows

Opens: C:\ProgramData\Microsoft\Windows\Caches

Opens: C:\Users
Opens: C:\Users\Admin

Opens: C:\Users\Admin\AppData
Opens: C:\Users\Admin\AppData\Roamin

Opens: C:\Users\Admin\AppData\Roaming
Opens: C:\Users\Admin\AppData\Roaming\Microsoft

Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows

Opens: C:\Users\Admin\AppData\Roaming\Microsoft\Windows\Start Menu

Opens: C:\Windows\AppPatch
Opens: C:\Windows\Globalization
Opens: C:\Windows\Globalization\Sorting

Opens: C:\Windows\inf

Reads from: C:\Windows\Prefetch\REGSVR32.EXE-8461DBEE.pf

Windows Registry Events

Creates key: HKLM\software\323546aeee592a07b90b

Creates key: HKLM\software\bfuhgx

Creates key: HKLM\software\microsoft\wbem\cimom

Deletes value: HKLM\software\323546aeee592a07b90b[530957d02ada99668870]

Deletes value: HKLM\software\bfuhgx[eay99xa]
Deletes value: HKLM\software\bfuhgx[wp2ccclpw]

Opens key: HKLM\system\currentcontrolset\control\session manager
Opens key: HKLM\system\currentcontrolset\control\safeboot\option
Opens key: HKLM\system\currentcontrolset\control\srp\gp\dll

Opens key: HKLM\software\policies\microsoft\windows\safer\codeidentifiers
Opens key: HKCU\software\policies\microsoft\windows\safer\codeidentifiers

Opens key: HKCU\

Opens key: HKCU\control panel\desktop\muicached\machinelanguageconfiguration

Opens key: HKLM\software\policies\microsoft\mui\settings
Opens key: HKCU\software\policies\microsoft\control panel\desktop
Opens key: HKCU\control panel\desktop\languageconfiguration

Opens key: HKCU\control panel\desktop

Opens key: HKCU\control panel\desktop\muicached

Opens key: HKLM\software\microsoft\windows\currentversion\sidebyside

Opens key:

HKLM\software\microsoft\windows\currentversion\sidebyside\assemblystorageroots
Opens key: HKLM\system\currentcontrolset\control\nls\sorting\versions
Opens key: HKLM\system\currentcontrolset\control\error message instrument\
Opens key: HKLM\system\currentcontrolset\control\error message instrument
Opens key: HKLM\software\microsoft\windows nt\currentversion\gre_initialize
Opens key: HKLM\software\microsoft\windows nt\currentversion\compatibility32
Opens key: HKLM\software\microsoft\windows nt\currentversion\ime compatibility

Opens key: HKLM\

Opens key: HKLM\software\microsoft\windows nt\currentversion\windows
Opens key: HKLM\software\microsoft\windows nt\currentversion\diagnostics
Opens key: HKLM\system\currentcontrol\set\control\nls\customlocale
Opens key: HKLM\system\currentcontrol\set\control\nls\extendedlocale

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions

Opens key: HKLM\software\microsoft\ole
Opens key: HKLM\software\microsoft\ole\tracing
Opens key:

 $HKLM\software\mbox{microsoft\windows\currentversion\explorer\folderdescriptions\folderd$

Opens key:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ property bag$

Opens key: HKCU\software\microsoft\windows\currentversion\explorer

 $Opens~key: \\ HKCU\software\microsoft\windows\currentversion\explorer\sessioninfo\label{eq:continuous}$

Opens key:

 $HKCU \ software \ `microsoft\ `windows \ `current version \ `explorer \ 's ession in folders' \ in the context of the contex$

Opens key: HKCU\software\microsoft\windows\currentversion\explorer\user shell folders

Opens key:

HKLM\software\microsoft\windows\currentversion\explorer\knownfoldersettings

Opens key: HKLM\system\currentcontrolset\control\nls\locale
Opens key: HKLM\system\currentcontrolset\control\nls\locale\alternate sorts

Opens key: HKLM\system\currentcontrolset\control\nls\language groups

Opens key: HKLM\software\microsoft\oleaut

Opens key: HKLM\system\currentcontrolset\services\crypt32

 $\label{lem:constant} Opens~key: $$ HKLM\software\microsoft\windows\currentversion\internet settings $$ Opens~key: $$ HKLM\software\policies\microsoft\windows\currentversion\internet $$ Opens~key: $$ Opens~key: $$ HKLM\software\policies\microsoft\windows\currentversion\internet $$ Opens~key: $$$

settings

Opens key: HKCU\software\borland\locales
Opens key: HKCU\software\borland\delphi\locales

Opens key: HKLM\software\policies\microsoft\sqmclient\windows

Opens key: HKLM\software\microsoft\sqmclient\windows

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters

Opens key: HKLM\system\currentcontrolset\services\winsock2\parameters\appid_catalog

Opens key:

 $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ appid_catalog \ 0d42e323$

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9

Opens key:

Opens kev:

 $HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters \setminus protocol_catalog 9 \setminus catalog_entries$

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000001
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000010

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011
Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012
Opens kev:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014
Opens key:

 $\label{lem:hklmsystem} HKLM \system \current controls et \services \winsock 2 \parameters \protocol_catalog 9 \catalog_entries \0000000000015 \parameters \end{substitute} Opens key:$

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000016
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017
Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018
Opens kev:

Opens kev:

Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries
 Opens key:

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001
Opens key:

Opens key: HKLM\software\microsoft\windows nt\currentversion

Opens key:

9305-67de0b28fc23}

Opens key:

9305-67de0b28fc23}\propertybag

Opens key: HKLM\software\

 Opens key:
 HKLM\software\323546aeee592a07b90b\

 Opens key:
 HKLM\software\323546aeee592a07b90b

Opens key: HKLM\software\bfuhgx
Opens key: HKLM\software\bfuhgx\
Opens key: HKLM\software\microsoft\rpc

Opens key: HKLM\system\currentcontrolset\control\computername\activecomputername

Opens key: HKLM\system\setup

Opens key: HKLM\software\policies\microsoft\windows nt\rpc

Opens key: HKCU\software\classes\

Opens key:

HKCU\software\classes\appid\677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5.exe

Opens kev:

HKCR\appid\677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5.exe

Opens key: HKLM\system\currentcontrolset\control\lsa

Opens key: HKLM\software\microsoft\com3

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}
Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\treatas

 Opens key:
 HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24\\treatas

 Opens key:
 HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f

00aa004b2e24}\progid

Opens key: $\begin{tabular}{ll} HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\progid\\ Opens key: \\ HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\end{tabular}$

00aa004b2e24}\inprocserver32

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprochandler32

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler32

Opens key: HKCU\software\classes\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprochandler

Opens key: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprochandler Opens key: HKLM\system\currentcontrolset\services\tcpip\parameters

Opens key: HKLM\software\policies\microsoft\system\dnsclient

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}
Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\treatas

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\treatas Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\progid

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\progid Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprocserver32

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprocserver32

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandler32

Opens key: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}\inprochandler32

Opens key: HKCU\software\classes\clsid\{8bc3f05e-d86b-11d0-a075-

00c04fb68820}\inprochandler

Opens key: $\label{eq:hkkcr} \mbox{HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820\}\inprochandler}$

Opens key: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

cryptographic provider

Opens key: HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy

Opens key:

Opens key: HKCU\software\classes\interface\{00000134-0000-0000-000000000046}

Opens key: HKCR\interface\{00000134-0000-0000-000000000046} Opens key: HKCU\software\classes\interface\{00000134-0000-0000-c000-

00000000046}\proxystubclsid32

Opens key: HKCR\interface\{00000134-0000-0000-c000-0000000046}\proxystubclsid32

Opens key: HKLM\software\microsoft\rpc\extensions
Opens key: HKLM\system\currentcontrolset\services\bfe

Opens key: HKLM\software\microsoft\sqmclient\windows\disabledprocesses\
Opens key: HKLM\software\microsoft\sqmclient\windows\disabledsessions\

Opens key: HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}

 Opens key:
 HKCR\interface\{f309ad18-d86a-11d0-a075-00c04fb68820}

 Opens key:
 HKCU\software\classes\interface\{f309ad18-d86a-11d0-a075

 ${\tt 00c04fb68820} \\ {\tt proxystubclsid32}$

Opens key: HKCR\interface\\{f309ad18-d86a-11d0-a075-00c04fb68820\\proxystubclsid32 Opens key: HKCU\software\classes\clsid\\{7c857801-7381-11cf-884d-00aa004b2e24\}

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}
Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\treatas

00aa004b2e24}\progid

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\progid Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\inprocserver32

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32

Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

 $00 a a 004 b 2 e 24 \} \\ \\ in prochandler 32$

Opens key: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprochandler32

Opens key: HKCU\software\classes\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\inprochandler

Opens key: $\label{eq:hkcr} \begin{tabular}{ll} HKCR\clsid\footnote{1.5}\clsid\footno$

Opens key: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}

HKCU\software\classes\interface\{d4781cd6-e5d3-44df-ad94-Opens key: 930efe48a887}\proxystubclsid32

HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32 Opens kev:

Opens key: HKLM\system\currentcontrolset\control\computername

Opens key: HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}

Opens key: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7} HKCU\software\classes\interface\{9556dc99-828c-11cf-a37e-Opens key:

00aa003240c7}\proxystubclsid32

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} Opens key:

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea} Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\treatas

HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\progid

Opens key: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\progid Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprocserver32

HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprochandler32

 $HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\tinprochandler 32$ Opens kev:

Opens key: HKCU\software\classes\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprochandler

HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprochandler Opens key:

Opens key: HKLM\software\microsoft\wbem\cimom

Opens key: HKCU\software\classes\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}

Opens key: HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24} Opens key: HKCU\software\classes\clsid\{4590f812-1d3a-11d0-891f-

00aa004b2e24}\treatas

HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\treatas Opens key: Opens key: HKCU\software\classes\clsid\{4590f812-1d3a-11d0-891f-

00aa004b2e24}\progid

HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\progid Opens key: Opens key: HKCU\software\classes\clsid\{4590f812-1d3a-11d0-891f-

00aa004b2e24}\inprocserver32

HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprocserver32 Opens key:

Opens key: HKCU\software\classes\clsid\{4590f812-1d3a-11d0-891f-

00aa004b2e24}\inprochandler32

HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprochandler32 Opens key:

Opens key:

00aa004b2e24}\inprochandler

HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}\inprochandler Opens key: Opens key: $HKCU \setminus software \setminus classes \setminus interface \setminus \{44aca675 - e8fc - 11d0 - a07c - 00c04fb68820\}$

Opens key: HKCR\interface\{44aca675-e8fc-11d0-a07c-00c04fb68820} HKCU\software\classes\interface\{44aca675-e8fc-11d0-a07c-Opens key:

00c04fb68820}\proxystubclsid32

HKCR\interface\{44aca675-e8fc-11d0-a07c-00c04fb68820}\proxystubclsid32 Opens kev: Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution options\regsvr32.exe

HKLM\system\currentcontrolset\control\session manager\appcertdlls Opens key: Opens key: HKLM\system\currentcontrolset\control\session manager\appcompatibility Opens key: HKLM\software\policies\microsoft\windows\appcompat

Opens kev: HKCU\software\microsoft\windows nt\currentversion

Opens key: HKCU\software\microsoft\windows nt\currentversion\appcompatflags\layers

Opens key: $\label{lem:hklm} \verb+Kklm \+ software + microsoft + windows + nt + current + version + approximately against the property of the software + microsoft + windows + nt + current + version + approximately + approximately + nt + current + version + approximately + approximate$

Opens key: HKLM\software\microsoft\windows nt\currentversion\appcompatflags\custom\regsvr32.exe

Opens key: HKLM\software\microsoft\windows nt\currentversion\image file execution

options

Queries value:

manager[cwdillegalindllsearch]

Oueries value:

HKLM\software\policies\microsoft\windows\safer\codeidentifiers[transparentenabled]

HKCU\control panel\desktop[preferreduilanguages] Oueries value:

Queries value: HKCU\control panel\desktop\muicached[machinepreferreduilanguages]

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side [preferex ternal manifest]] \ details a side by side by side by side [preferex ternal manifest]] \ details a side by sid$ HKLM\system\currentcontrolset\control\nls\sorting\versions[] Oueries value:

Queries value: HKLM\system\currentcontrolset\control\session manager[safedllsearchmode]

Queries value: HKLM\software\microsoft\windows nt\currentversion\gre_initialize[disablemetafiles] Queries value: HKLM\software\microsoft\windows

nt\currentversion\compatibility32[677926883abd5e9e34c0ac6435a9272a3be5efc9ab7e97c5e01b12b6e5d75fb5]

Oueries value: HKLM\software\microsoft\windows

nt\currentversion\windows[loadappinit_dlls]

HKLM\system\currentcontrolset\control\nls\customlocale[en-us] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-us] Oueries value: HKLM\software\microsoft\ole[pageallocatorusesystemheap] Queries value: HKLM\software\microsoft\ole[pageallocatorsystemheapisprivate] Oueries value:

b029-7fe99a87c641}[category]

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [name]$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows} Learned the substitution of the substitutio$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ [description]$

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [relative path]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ (b4bfcc3a-db2c-424c-b029-7fe99a87c641) \ [parsing name]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [infotip]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[localized name]$

Oueries value:

 $\label{lem:hklmsoftware} Hklm\software\microsoft\windows\currentversion\explorer\folderdescriptions\folder$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ (b4bfcc3a-db2c-424c-b029-7fe99a87c641) \ [security]$

Oueries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[stream resource]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ [stream resource type]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ [local redirectonly]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ [roamable]$

Oueries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ [precreate]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} [stream]$

Queries value:

 $HKLM \ software \ microsoft \ windows \ current version \ \ explorer \ folder descriptions \ \{b4bfcc3a-db2c-424c-b029-7fe99a87c641\} \ [publish \ explorer\]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[attributes]$

Queries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}\[foldertypeid]\]$

Queries value:

 $\label{lem:hklmsoftwaremicrosoftwindows\currentversion\explorer\folderdescriptions\{b4bfcc3a-db2c-424c-b029-7fe99a87c641\}[initfolderhandler]} \\$

Queries value: HKCU\software\microsoft\windows\currentversion\explorer\user shell

folders[desktop]

Queries value: HKLM\system\currentcontrolset\control\session

manager[safeprocesssearchmode]

HKLM\system\currentcontrolset\control\nls\customlocale[ar] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ar] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ar-sa] HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-sa] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[bg] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[bg] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[bg-bg] HKLM\system\currentcontrolset\control\nls\extendedlocale[bg-bg] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ca] HKLM\system\currentcontrolset\control\nls\extendedlocale[ca] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ca-es] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ca-es] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[zh-hans] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-hans] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[zh-cn] HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-cn] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[cs] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[cs] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[cs-cz] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[cs-cz] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[da]

HKLM\system\currentcontrolset\control\nls\extendedlocale[da] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[da-dk] Oueries value: Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[de] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[de] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[de-de] HKLM\system\currentcontrolset\control\nls\extendedlocale[de-de] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ell Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[el] HKLM\system\currentcontrolset\control\nls\customlocale[el-gr] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[el-gr] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[es] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es] HKLM\system\currentcontrolset\control\nls\customlocale[es-es] Oueries value: Oueries value: HKI M\system\currentcontrolset\control\nls\extendedlocale[es-es] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[fi] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fi] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fi-fi] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fi-fi] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fr] HKLM\system\currentcontrolset\control\nls\extendedlocale[fr] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fr-fr] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[he] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[he] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[he-il] HKLM\system\currentcontrolset\control\nls\extendedlocale[he-il] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[hu] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hu] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[hu-hu] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hu-hu] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[is] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[is] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[is-is] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[is-is] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[it] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[it] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[it-it] HKLM\system\currentcontrolset\control\nls\extendedlocale[it-it] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ja] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ja] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ja-jp] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ja-jp] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ko] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ko] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ko-kr] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ko-kr] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[nl] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[nl] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[nl-nl] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[nl-nl] HKLM\system\currentcontrolset\control\nls\customlocale[no] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[no] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[nb-no] HKLM\system\currentcontrolset\control\nls\extendedlocale[nb-no] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[pl] HKLM\system\currentcontrolset\control\nls\extendedlocale[pl] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[pl-pl] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[pl-pl] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[pt] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[pt] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[pt-br] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[pt-br] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[rm] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[rm] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[rm-ch] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[rm-ch] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ro] HKLM\system\currentcontrolset\control\nls\extendedlocale[ro] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ro-ro] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ro-ro] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ru] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ru] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ru-ru] $HKLM \verb|\system| current controlset \verb|\control| nls \verb|\extended| locale[ru-ru]|$ Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[hr] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hrl Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[hr-hr] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hr-hr] HKLM\system\currentcontrolset\control\nls\customlocale[sk] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sk]

HKLM\system\currentcontrolset\control\nls\customlocale[sk-sk] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sk-sk] Oueries value: $HKLM \verb|\system| current controlset| control \verb|\nls| custom locale[sq]|$ Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sq] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sq-al] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sq-al] HKLM\system\currentcontrolset\control\nls\customlocale[sv] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sv] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[sv-se] HKLM\system\currentcontrolset\control\nls\extendedlocale[sv-se] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[th] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[th] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[th-th] Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[th-th] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[tr] HKLM\system\currentcontrolset\control\nls\extendedlocale[tr] Oueries value: Oueries value: HKI M\system\currentcontrolset\control\nls\customlocale[tr-tr] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tr-tr] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ur] HKLM\system\currentcontrolset\control\nls\extendedlocale[ur] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ur-pk] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ur-pk] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[id] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[id] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[id-id] HKLM\system\currentcontrolset\control\nls\extendedlocale[id-id] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[uk] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[uk] HKLM\system\currentcontrolset\control\nls\customlocale[uk-ua] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[uk-ua] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[be] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[be] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[be-by] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[be-by] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[sl] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sl] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[sl-si] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sl-si] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[et] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[et] HKLM\system\currentcontrolset\control\nls\customlocale[et-ee] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[et-ee] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[lv] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[lv] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[lv-lv] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[lv-lv] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[lt] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[lt-lt] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[lt-lt] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[tg] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tg] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[tg-cyrl-tj] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tg-cyrl-tj] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fa] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fa] HKLM\system\currentcontrolset\control\nls\customlocale[fa-ir] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fa-ir] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[vi] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[vi] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[vi-vn] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[vi-vn] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[hy] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hy] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[hy-am] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hy-am] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[az] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[az] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[az-latn-az] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[az-latn-az] $HKLM \verb|\system| current controlset| control \verb|\nls| custom locale[eu]|$ Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[eu] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[eu-es] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[eu-es] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[hsb] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hsb] $HKLM \verb|\system| current controls et \verb|\control| nls \verb|\custom| locale [hsb-de]|$ Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hsb-de] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[mkl Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mk] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[mk-mk] HKLM\system\currentcontrolset\control\nls\extendedlocale[mk-mk] Oueries value: Queries value:

HKLM\system\currentcontrolset\control\nls\extendedlocale[tn] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[tn-zal Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tn-za] HKLM\system\currentcontrolset\control\nls\customlocale[xh] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[xh] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[xh-za] HKLM\system\currentcontrolset\control\nls\extendedlocale[xh-za] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[zu] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[zu] HKLM\system\currentcontrolset\control\nls\customlocale[zu-za] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[zu-za] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[af] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[af] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[af-zal Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[af-za] HKLM\system\currentcontrolset\control\nls\customlocale[ka] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ka] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ka-ge] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ka-ge] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fo] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fo] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fo-fo] HKLM\system\currentcontrolset\control\nls\extendedlocale[fo-fo] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[hi] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hi] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[hi-in] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hi-in] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[mt] Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[mt] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[mt-mt] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mt-mt] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[se] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[se] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[se-no] HKLM\system\currentcontrolset\control\nls\extendedlocale[se-no] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ga] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ga] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ga-ie] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ga-ie] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ms] $HKLM \verb|\system| current controlset| control \verb|\nls| extended locale[ms]|$ Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ms-my] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ms-my] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[kk] HKLM\system\currentcontrolset\control\nls\extendedlocale[kk] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[kk-kz] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[kk-kz] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ky] HKLM\system\currentcontrolset\control\nls\extendedlocale[ky] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ky-kg] HKLM\system\currentcontrolset\control\nls\extendedlocale[ky-kg] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[sw] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sw] HKLM\system\currentcontrolset\control\nls\customlocale[sw-ke] Queries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[sw-ke] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[tk] HKLM\system\currentcontrolset\control\nls\extendedlocale[tk] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[tk-tm] HKLM\system\currentcontrolset\control\nls\extendedlocale[tk-tm] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[uz] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[uz] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[uz-latn-uz] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[tt] HKLM\system\currentcontrolset\control\nls\extendedlocale[tt] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[tt-ru] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tt-ru] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[bn] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[bn-in] ${\tt HKLM \ } system \verb|\ current control \ | \ lextended \ locale [bn-in]$ Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[pa] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[pa] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[pa-in] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[pa-in] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[gu] $HKLM \verb|\system| current controls et \verb|\control| nls \verb|\extended locale[gu]|$ Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[gu-in] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gu-in] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[or] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[or] Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[or-in] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[or-in]

HKLM\system\currentcontrolset\control\nls\customlocale[ta] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tal Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ta-in] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ta-in] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[te] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[te] HKLM\system\currentcontrolset\control\nls\customlocale[te-in] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[te-in] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[kn] HKLM\system\currentcontrolset\control\nls\extendedlocale[kn] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[kn-in] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[kn-in] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ml] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ml] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ml-in] HKLM\system\currentcontrolset\control\nls\extendedlocale[ml-in] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[as] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[as] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[as-in] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[as-in] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[mr] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mr] HKLM\system\currentcontrolset\control\nls\customlocale[mr-in] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mr-in] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sa] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sa] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[sa-in] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sa-in] Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[mn] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mn] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[mn-mn] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mn-mn] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[bo] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[bo] HKLM\system\currentcontrolset\control\nls\customlocale[bo-cn] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[bo-cn] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[cy] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[cy] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[cy-gb] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[cy-gb] $HKLM \verb|\system| current controlset| control \verb|\nls| custom locale[km]|$ Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[km] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[km-kh] HKLM\system\currentcontrolset\control\nls\extendedlocale[km-kh] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[lo] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[lo] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[lo-la] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[lo-la] HKLM\system\currentcontrolset\control\nls\customlocale[gl] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gl] HKLM\system\currentcontrolset\control\nls\customlocale[gl-es] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gl-es] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[kok] HKLM\system\currentcontrolset\control\nls\extendedlocale[kok] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[kok-in] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[kok-in] HKLM\system\currentcontrolset\control\nls\customlocale[syr] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[syr] HKLM\system\currentcontrolset\control\nls\customlocale[syr-sy] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[syr-sy] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[si] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[si] HKLM\system\currentcontrolset\control\nls\customlocale[si-lk] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[si-lk] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[iu] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[iu] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[iu-latn-ca] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[iu-latn-ca] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[am] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[am] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[am-et] HKLM\system\currentcontrolset\control\nls\extendedlocale[am-et] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[tzm] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tzm] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[tzm-latn-dz] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tzm-latn-dz] $HKLM \verb|\system| current controlset| control \verb|\nls| custom locale[ne]|$ Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ne] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ne-np] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ne-np] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[fy] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fv] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[fy-nl]

HKLM\system\currentcontrolset\control\nls\extendedlocale[fy-nl] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ps] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ps] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ps-af] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ps-af] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[fil] HKLM\system\currentcontrolset\control\nls\extendedlocale[fil] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fil-ph] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fil-ph] HKLM\system\currentcontrolset\control\nls\customlocale[dv] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[dv] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[dv-mv] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[dv-mv] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[hal Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ha] HKLM\system\currentcontrolset\control\nls\customlocale[ha-latn-ng] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ha-latn-ng] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[yo] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[yo] HKLM\system\currentcontrolset\control\nls\customlocale[yo-ng] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[yo-ng] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[quz] HKLM\system\currentcontrolset\control\nls\extendedlocale[quz] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[quz-bo] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[quz-bo] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[nso] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[nso] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[nso-za] HKLM\system\currentcontrolset\control\nls\extendedlocale[nso-za] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ba] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ba] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ba-ru] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ba-ru] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[lb] HKLM\system\currentcontrolset\control\nls\extendedlocale[lb] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[lb-lu] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[lb-lu] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[kl] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[kl] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[kl-gl] HKLM\system\currentcontrolset\control\nls\extendedlocale[kl-gl] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ig] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ig] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ig-ng] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ig-ng] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ii] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ii] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ii-cn] HKLM\system\currentcontrolset\control\nls\extendedlocale[ii-cn] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[arn] HKLM\system\currentcontrolset\control\nls\extendedlocale[arn] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[arn-cl] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[arn-cl] HKLM\system\currentcontrolset\control\nls\customlocale[moh] Queries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[moh] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[moh-ca] HKLM\system\currentcontrolset\control\nls\extendedlocale[moh-ca] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[br] HKLM\system\currentcontrolset\control\nls\extendedlocale[br] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[br-fr] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[br-fr] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ug] HKLM\system\currentcontrolset\control\nls\extendedlocale[ug] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ug-cn] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ug-cn] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[mi] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mi] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[mi-nz] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mi-nz] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[oc] $HKLM \verb|\system| current controlset| control \verb|\nls| extended locale[oc]|$ Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[oc-fr] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[oc-fr] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[co] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[co] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[co-fr] $HKLM \verb|\system| current controlset \verb|\control| nls \verb|\extended| locale [co-fr]|$ Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[gsw] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gswl Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[gsw-fr] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gsw-fr] HKLM\system\currentcontrolset\control\nls\customlocale[sah] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sah]

HKLM\system\currentcontrolset\control\nls\customlocale[sah-ru] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sah-rul Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[qut] HKLM\system\currentcontrolset\control\nls\extendedlocale[qut] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[gut-gt] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[qut-gt] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[rw] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[rw] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[rw-rw] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[rw-rw] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[wol Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[wo] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[wo-sn] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[wo-sn] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[prs] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[prs] HKLM\system\currentcontrolset\control\nls\customlocale[prs-af] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[prs-af] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[gd] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gd] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[gd-gb] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[gd-gb] HKLM\system\currentcontrolset\control\nls\locale[00000401] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\language groups[d] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000402] Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[5] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000403] Queries value: HKLM\system\currentcontrolset\control\nls\language groups[1] Queries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[zh-tw] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-tw] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000404] Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[9] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000405] Queries value: HKLM\system\currentcontrolset\control\nls\language groups[2] HKLM\system\currentcontrolset\control\nls\locale[00000406] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000407] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000408] Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[4] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000409] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-es_tradnl] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es-es_tradnl] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000040b] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000040c] HKLM\system\currentcontrolset\control\nls\locale[0000040d] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\language groups[c] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000040e] Queries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\locale[00000410] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000411] HKLM\system\currentcontrolset\control\nls\language groups[7] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\localef000004121 Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[8] HKLM\system\currentcontrolset\control\nls\locale[00000413] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000414] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000415] $HKLM \ system \ current controls et \ control \ nls \ locale [00000416]$ Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000417] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000418] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000419] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000041a] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000041b] HKLM\system\currentcontrolset\control\nls\locale[0000041c] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000041d] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000041e] Queries value: HKLM\system\currentcontrolset\control\nls\language groups[b] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000041f] Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[6] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000421] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000422] HKLM\system\currentcontrolset\control\nls\locale[00000423] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000424] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000425] Queries value: HKLM\system\currentcontrolset\control\nls\language groups[3] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000426] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000427] HKLM\system\currentcontrolset\control\nls\locale[00000428] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000429] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000042a] Queries value: HKLM\system\currentcontrolset\control\nls\language groups[e] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000042b] Queries value: HKLM\system\currentcontrolset\control\nls\language groups[11]

Oueries value:

HKLM\system\currentcontrolset\control\nls\locale[0000042d] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000042e] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000042f] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000432] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000435] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[000004361 Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000437] Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[10] HKLM\system\currentcontrolset\control\nls\locale[00000438] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000439] Oueries value: HKLM\system\currentcontrolset\control\nls\language groups[f] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000043a] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000043b] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000043e] Oueries value: HKLM\svstem\currentcontrolset\control\nls\locale[0000043f] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000440] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000441] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000442] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000443] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000444] Oueries value: HKLM\svstem\currentcontrolset\control\nls\locale[00000445] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000446] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000447] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000448] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000449] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000044a] Oueries value: HKLM\svstem\currentcontrolset\control\nls\locale[0000044b] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000044c] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000044d] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000044e] HKLM\system\currentcontrolset\control\nls\locale[0000044f] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000450] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000451] Queries value: Queries value: HKLM\svstem\currentcontrolset\control\nls\localef000004531 Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000454] HKLM\system\currentcontrolset\control\nls\locale[00000456] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000457] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000045a] $HKLM \verb|\system| current controlset| control \verb|\nls|| locale [0000045b]|$ Queries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[iu-cans-ca] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[iu-cans-ca] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000045e] Oueries value: Queries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\locale[00000463] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000464] $HKLM \verb|\system| current controlset| control \verb|\nls|| locale [00000465]$ Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000468] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000046a] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000046b] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000046c] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000046d] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000046e] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000046f] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000470] HKLM\system\currentcontrolset\control\nls\locale[00000478] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000047a] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000047c] $HKLM \verb|\system| current controlset| control \verb|\nls|| locale[0000047e]$ Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000480] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000481] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000483] Oueries value: Queries value: $HKLM \verb|\system| current controlset| control \verb|\nls|| locale [00000485]|$ Oueries value: HKLM\svstem\currentcontrolset\control\nls\locale[00000486] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000487] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000048c] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000491] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[qps-ploc] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[aps-ploc] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000501] HKLM\system\currentcontrolset\control\nls\locale\alternate Oueries value: sorts[00000501] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[qps-ploca]

 $HKLM \ system \ current control set \ control \ nls \ locale [0000042c]$

Oueries value:

Queries value: HKLM\system\currentcontrol\set\control\nls\customlocale[qps-ploca]

Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[qps-ploca]

Queries value: HKLM\system\currentcontrolset\control\nls\locale[000005fe]

Queries value: HKLM\system\currentcontrolset\control\nls\locale\oldaybelaternate

Queries value: HKLM\system\currentcontrolset\control\nls\locale\alternate

sorts[000005fe]

HKLM\system\currentcontrolset\control\nls\customlocale[ar-iq] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-iq] HKLM\system\currentcontrolset\control\nls\locale[00000801] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000804] Queries value: HKLM\system\currentcontrolset\control\nls\language groups[a] HKLM\system\currentcontrolset\control\nls\customlocale[de-ch] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[de-ch] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000807] HKLM\system\currentcontrolset\control\nls\customlocale[en-gb] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en-gb] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000809] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-mx] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es-mx] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000080a] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fr-be] HKLM\system\currentcontrolset\control\nls\extendedlocale[fr-be] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000080c] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[it-ch] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[it-ch] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000810] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[nl-be] Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[nl-be] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000813] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[nn-no] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[nn-no] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000814] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[pt-pt] Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[pt-pt] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000816] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[sr-latn-cs] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-latn-cs] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000081a] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[sv-fi] HKLM\system\currentcontrolset\control\nls\extendedlocale[sv-fi] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000081d] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[az-cyrl-az] HKLM\system\currentcontrolset\control\nls\extendedlocale[az-cyrl-az] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000082c] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[dsb-de] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[dsb-de] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000082e] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[se-se] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[se-se] HKLM\system\currentcontrolset\control\nls\locale[0000083b] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000083c] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ms-bn] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ms-bn] Oueries value: HKLM\svstem\currentcontrolset\control\nls\locale[0000083e] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[uz-cyrl-uz] HKLM\system\currentcontrolset\control\nls\extendedlocale[uz-cyrl-uz] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000843] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[bn-bd] HKLM\system\currentcontrolset\control\nls\extendedlocale[bn-bd] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[000008451 Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[mn-mong-cn] HKLM\system\currentcontrolset\control\nls\extendedlocale[mn-mong-cn] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000850] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000085d] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000085f] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[quz-ec] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[quz-ec] HKLM\system\currentcontrolset\control\nls\locale[0000086b] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[qps-plocm] HKLM\system\currentcontrolset\control\nls\extendedlocale[qps-plocm] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[000009ff] Queries value: HKLM\system\currentcontrolset\control\nls\locale\alternate Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[ar-eg]

sorts[000009ff1

HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-eg] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000c01] HKLM\system\currentcontrolset\control\nls\customlocale[zh-hk] Oueries value: Queries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[zh-hkl Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000c04] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[de-at] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[de-at] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000c07] HKLM\system\currentcontrolset\control\nls\customlocale[en-au] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en-aul Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00000c09] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00000c0a] Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[fr-ca] Queries value:

HKLM\system\currentcontrolset\control\nls\locale[00000c0c] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sr-cvrl-csl Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-cyrl-cs] HKLM\system\currentcontrolset\control\nls\locale[00000c1a] Queries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[se-fil Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[se-fi] HKLM\system\currentcontrolset\control\nls\locale[00000c3b] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[guz-pel Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[quz-pe] HKLM\system\currentcontrolset\control\nls\locale[00000c6b] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[ar-lv] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-ly] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00001001] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[zh-sg] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-sg] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00001004] Queries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[de-lu] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[de-lu] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00001007] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-ca] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-ca] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00001009] Queries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[es-gt] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es-gt] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000100a] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fr-ch] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fr-ch] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000100c] Queries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[hr-ba] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[hr-ba] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000101a] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[smj-no] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[smj-no] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000103b] HKLM\system\currentcontrolset\control\nls\customlocale[ar-dz] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-dz] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00001401] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[zh-mo] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-mo] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00001404] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[de-li] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[de-li] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00001407] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-nz] HKLM\system\currentcontrolset\control\nls\extendedlocale[en-nz] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00001409] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-cr] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es-cr] Oueries value: HKLM\svstem\currentcontrolset\control\nls\locale[0000140a] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[fr-lu] HKLM\system\currentcontrolset\control\nls\extendedlocale[fr-lu] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000140c] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[bs-latn-ba] HKLM\system\currentcontrolset\control\nls\extendedlocale[bs-latn-ba] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000141a] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[smj-se] HKLM\system\currentcontrolset\control\nls\extendedlocale[smj-se] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000143b] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ar-ma] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-ma] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00001801] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-ie] HKLM\system\currentcontrolset\control\nls\extendedlocale[en-ie] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00001809] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-pa] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es-pa] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000180a] Oueries value: $HKLM \verb|\system| current controlset| \verb|\control| nls| custom locale[fr-mc]|$ Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[fr-mc] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000180c] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sr-latn-ba] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[0000181a] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sma-no] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sma-no] HKLM\system\currentcontrolset\control\nls\locale[0000183b] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ar-tn] HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-tn] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00001c01] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-za] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[en-za] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00001c09] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-do]

```
HKLM\system\currentcontrolset\control\nls\extendedlocale[es-do]
Oueries value:
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\localef00001c0al
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[sr-cyrl-ba]
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-cyrl-ba]
Queries value:
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00001c1a]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[sma-se]
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[sma-se]
Oueries value:
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\localef00001c3bl
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[ar-om]
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-om]
Oueries value:
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00002001]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[en-jm]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[en-jm]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00002009]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[es-ve]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[es-ve]
                       HKLM\system\currentcontrolset\control\nls\locale[0000200a]
Queries value:
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[bs-cyrl-ba]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[bs-cyrl-ba]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[0000201a]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[sms-fi]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[sms-fi]
                       HKLM\system\currentcontrolset\control\nls\locale[0000203b]
Queries value:
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[ar-ye]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-ye]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00002401]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[en-029]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[en-029]
Queries value:
                       HKLM\svstem\currentcontrolset\control\nls\locale[00002409]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[es-co]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[es-co]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[0000240a]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[sr-latn-rs]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-latn-rs]
                       HKLM\system\currentcontrolset\control\nls\locale[0000241a]
Oueries value:
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[smn-fi]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[smn-fi]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[0000243b]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[ar-sy]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-sy]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00002801]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[en-bz]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[en-bz]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00002809]
                       HKLM\system\currentcontrolset\control\nls\customlocale[es-pe]
Oueries value:
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[es-pe]
Oueries value:
                       Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[sr-cyrl-rs]
Oueries value:
                       HKLM\svstem\currentcontrolset\control\nls\extendedlocale[sr-cvrl-rs]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[0000281a]
                       HKLM\system\currentcontrolset\control\nls\customlocale[ar-jo]
Oueries value:
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-io1
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00002c01]
                       HKLM\system\currentcontrolset\control\nls\customlocale[en-tt]
Queries value:
Oueries value:
                       HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en-tt]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00002c09]
                       HKLM\system\currentcontrolset\control\nls\customlocale[es-ar]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[es-ar]
Oueries value:
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00002c0a]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[sr-latn-me]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-latn-me]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00002c1a]
                       HKLM\system\currentcontrolset\control\nls\customlocale[ar-lb]
Queries value:
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-lb]
                       HKLM\system\currentcontrolset\control\nls\locale[00003001]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[en-zw]
Oueries value:
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[en-zw]
Oueries value:
                       Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[es-ec]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[es-ec]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[0000300a]
                       HKLM\system\currentcontrolset\control\nls\customlocale[sr-cyrl-me]
Oueries value:
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-cvrl-me]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[0000301a]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[ar-kw]
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-kw]
Oueries value:
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00003401]
                       HKLM\system\currentcontrolset\control\nls\customlocale[en-ph]
Oueries value:
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\extendedlocale[en-ph]
Oueries value:
                       HKLM\system\currentcontrolset\control\nls\locale[00003409]
Queries value:
                       HKLM\system\currentcontrolset\control\nls\customlocale[es-cl]
Oueries value:
                       HKLM\svstem\currentcontrolset\control\nls\extendedlocale[es-cl]
Queries value:
```

HKLM\system\currentcontrolset\control\nls\customlocale[ar-ae] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[ar-ael Queries value: HKLM\system\currentcontrolset\control\nls\locale[00003801] HKLM\system\currentcontrolset\control\nls\customlocale[es-uy] Queries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[es-uv] Queries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ar-bh] Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[ar-bh] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00003c01] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-py] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es-py] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00003c0a] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[ar-qa] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[ar-ga] Oueries value: HKLM\system\currentcontrolset\control\nls\locale[00004001] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-in] Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en-in] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00004009] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-bo] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es-bo] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000400a] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-my] Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[en-mv] Queries value: HKLM\system\currentcontrolset\control\nls\locale[00004409] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-sv] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es-sv] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000440a] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[en-sg] HKLM\system\currentcontrolset\control\nls\extendedlocale[en-sg] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\locale[00004809] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-hn] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es-hn] Queries value: HKLM\system\currentcontrolset\control\nls\locale[0000480a] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-ni] Oueries value: Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-pr] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es-pr] HKLM\system\currentcontrolset\control\nls\locale[0000500a] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[es-us] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[es-us] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[bs-cyrl] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[bs-cyrl] HKLM\system\currentcontrolset\control\nls\customlocale[bs-latn] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[bs-latn] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sr-cyrl] Queries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[sr-latn] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sr-latn] HKLM\system\currentcontrolset\control\nls\customlocale[smn] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[smn] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[az-cyrl] HKLM\system\currentcontrolset\control\nls\extendedlocale[az-cyrl] Queries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[sms] Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[sms] $\label{lem:hklmsystem} \\ \text{HKLM} \\ \text{System} \\ \text{current control set} \\ \text{control } \\ \text{nls} \\ \text{custom locale} \\ \text{[zh]} \\$ Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[zh] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[nn] HKLM\system\currentcontrolset\control\nls\extendedlocale[nn] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[bs] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[bs] HKLM\system\currentcontrolset\control\nls\customlocale[az-latn] Queries value: Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[az-latn] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sma] HKLM\system\currentcontrolset\control\nls\extendedlocale[sma] Oueries value: Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[uz-cyrl] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[uz-cyrl] Queries value: $HKLM \setminus system \setminus current control \setminus nls \setminus custom locale [mn-cyrl]$ Queries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[mn-cyrl] Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[iu-cans] HKLM\system\currentcontrolset\control\nls\extendedlocale[iu-cans] Oueries value: Oueries value: HKLM\svstem\currentcontrolset\control\nls\customlocale[zh-hant] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[zh-hant] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[nb] HKLM\system\currentcontrolset\control\nls\extendedlocale[nb] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[sr] HKLM\system\currentcontrolset\control\nls\extendedlocale[sr] Oueries value: Oueries value: HKLM\system\currentcontrolset\control\nls\customlocale[tg-cyrl] Oueries value: HKLM\system\currentcontrolset\control\nls\extendedlocale[tg-cyrl] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[dsb] Oueries value: HKLM\svstem\currentcontrolset\control\nls\extendedlocale[dsb] Queries value: HKLM\system\currentcontrolset\control\nls\customlocale[smj]

```
Oueries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[smj]
                     HKLM\svstem\currentcontrolset\control\nls\customlocale[uz-latn]
 Oueries value:
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[uz-latn]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[mn-mong]
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[mn-mong]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[iu-latn]
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[iu-latn]
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[tzm-latn]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[tzm-latn]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[ha-latn]
 Oueries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[ha-latn]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\customlocale[]
 Queries value:
                     HKLM\system\currentcontrolset\control\nls\extendedlocale[]
                     HKLM\system\currentcontrolset\services\crypt32[debugheapflags]
 Oueries value:
 Queries value:
                     HKLM\software\microsoft\windows\currentversion\internet
settings[disableimprovedzonecheck]
                     HKLM\software\policies\microsoft\windows\currentversion\internet
 Oueries value:
settings[security_hklm_only]
                     HKLM\software\microsoft\sqmclient\windows[ceipenable]
 Queries value:
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters[winsock_registry_version]
 Queries value:
HKLM \setminus system \setminus current control set \setminus services \setminus winsock 2 \setminus parameters [namespace\_callout]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9[serial_access_num]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000001[packedcatalogitem]
 Queries value:
Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000004[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000005[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\00000000007[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000008[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000010[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000011[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000012[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000013[packedcatalogitem]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000014[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000015[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000016[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000017[packedcatalogitem]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\protocol_catalog9\catalog_entries\000000000018[packedcatalogitem]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[serial_access_num]
 Queries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5[num_catalog_entries]
 Oueries value:
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[librarypath]
HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[displaystring]
 Queries value:
```

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[addressfamily]

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog \ set alog_entries \ (0000000000001[version]) \ details \ de$

HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000001[supportednamespace]

Oueries value:

Oueries value:

Queries value:

Oueries value:

Oueries value:

- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[storesserviceclassinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000001[providerinfo]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[librarypath] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[displaystring] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[supportednamespace]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000002[storesserviceclassinfo]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000002[providerinfo] Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[displaystring]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ namespace_catalog \ solves \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[supportednamespace]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[enabled] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[version]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000003[storesserviceclassinfo]
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000003[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[librarypath]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\0000000000004[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000004[enabled]
 Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog5 \catalog_entries \000000000004 \[version] \queries \value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000004[providerinfo]
 Queries value:
- $HKLM \ system \ current control set \ services \ winsock 2 \ parameters \ names pace_catalog 5 \ catalog_entries \ 0000000000005 [library path] \ Oueries \ value:$
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[displaystring]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerid]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[addressfamily]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[supportednamespace]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000005[enabled]
 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[version]

 Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[storesserviceclassinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000005[providerinfo] Oueries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[librarypath]
 Queries value:
- HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[displaystring] Queries value:
- $\label{lem:hklmsystem} HKLM \system \current controlset \services \winsock 2 \parameters \namespace_catalog \shape \current \shape \s$

 $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000006 \ [address family]$ Oueries value: $HKLM \ system \ (current control set \ services \ winsock 2 \ parameters \ name space_catalog 5 \ (catalog_entries \ 0000000000006 [supported name space]]$ Queries value: Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\000000000006[version] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog_entries\00000000006[storesserviceclassinfo] Oueries value: HKLM\system\currentcontrolset\services\winsock2\parameters\namespace_catalog5\catalog_entries\00000000006[providerinfo] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32numhandlebuckets] Queries value: HKLM\system\currentcontrolset\services\winsock2\parameters[ws2_32spincount] HKLM\software\microsoft\windows nt\currentversion[installdate] Queries value: Oueries value: 9305-67de0b28fc23}[category] Queries value: 9305-67de0b28fc23}[name] Oueries value: 9305-67de0b28fc23}[parentfolder] Queries value: 9305-67de0b28fc23}[description] Oueries value: 9305-67de0b28fc23}[relativepath] Queries value: 9305-67de0b28fc23}[parsingname] Oueries value: 9305-67de0b28fc23}[infotip] Queries value: 9305-67de0b28fc23}[localizedname] Oueries value: 9305-67de0b28fc23}[icon1 Queries value: 9305-67de0b28fc23}[security] Oueries value: 9305-67de0b28fc23}[streamresource] Queries value: HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23}[streamresourcetype] Queries value: 9305-67de0b28fc23}[localredirectonly] Queries value:

Queries value:

 $\label{lem:hkkm} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fi38bf404-1d43-42f2-9305-67de0b28fc23\[precreate]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f38bf404-1d43-42f2-9305-67de0b28fc23\} \ [stream]$

Queries value:

 $\label{lem:hklmsoftware} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\fifth{1}{638bf404-1d43-42f2-9305-67de0b28fc23}\[publishexpandedpath]$

Queries value:

 $\label{lem:hamilton} HKLM\software\microsoft\windows\currentversion\explorer\folderdescriptions\{f38bf404-1d43-42f2-9305-67de0b28fc23\}[attributes]}$

Queries value:

 $\label{thm:local-prop} HKLM \software \microsoft \windows \current version \explorer \folder descriptions \fi38bf404-1d43-42f2-9305-67de0b28fc23 \folder typeid\]$

Queries value:

 $HKLM \ software \ `microsoft \ 'windows \ 'current version \ 'explorer \ 'folder descriptions \ '\{f38bf404-1d43-42f2-9305-67de0b28fc23\}[init folder handler]$

Queries value: HKLM\software\323546aeee592a07b90b[530957d02ada99668870]

Queries value: HKLM\software\bfuhgx[wp2ccclpw]
Queries value: HKLM\software\microsoft\rpc[maxrpcsize]

Queries value:

Queries value: HKLM\system\setup[oobeinprogress]
Queries value: HKLM\system\setup[systemsetupinprogress]

Queries value: HKLM\system\currentcontrolset\control\lsa[everyoneincludesanonymous]

Queries value: HKLM\software\microsoft\com3[com+enabled]

Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}[]

Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-00aa004b2e24}\inprocserver32[]

Queries value: HKCR\clsid\{4590f811-1d3a-11d0-891f-

00aa004b2e24}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\ole[maxsxshashcount]

Queries value: HKLM\software\microsoft\wbem\cimom[logging directory]

Queries value: HKLM\software\microsoft\wbem\cimom[logging]

Queries value: HKLM\software\microsoft\wbem\cimom[log file max size]

Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[hostname] Queries value: HKLM\system\currentcontrolset\services\tcpip\parameters[domain]

Queries value: HKCR\clsid\{8bc3f05e-d86b-11d0-a075-00c04fb68820}[]

Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

cryptographic provider[type]

Queries value: HKLM\software\microsoft\cryptography\defaults\provider\microsoft strong

cryptographic provider[image path]

 Queries value:
 HKLM\system\currentcontrolset\control\lsa\fipsalgorithmpolicy[enabled]

 Queries value:
 HKLM\system\currentcontrolset\control\lsa[fipsalgorithmpolicy]

 Queries value:
 HKLM\software\policies\microsoft\cryptography[privkeycachemaxitems]

Queries value:

HKLM\software\policies\microsoft\cryptography[privkeycachepurgeintervalseconds]

Queries value: HKLM\software\policies\microsoft\cryptography[privatekeylifetimeseconds]

Queries value: HKLM\software\microsoft\cryptography[machineguid]

Queries value: HKCR\interface\{00000134-0000-0000-0000000000046}\proxystubclsid32[]

Queries value: HKLM\software\microsoft\rpc\extensions[ndroleextdll]
Queries value: HKLM\software\microsoft\rpc\extensions[remoterpcdll]

Queries value: HKLM\software\microsoft\sqmclient\windows\disabledprocesses[a55708c0]

Queries value:

HKLM\software\microsoft\sqmclient\windows\disabledsessions[machinethrottling]

Queries value:

HKLM\software\microsoft\sqmclient\windows\disabledsessions[globalsession]

Queries value: HKLM\software\microsoft\ole[maximumallowedallocationsize]

Queries value: HKCR\interface\\\ f309ad18-d86a-11d0-a075-00c04fb68820\\\\ proxystubclsid32[]

Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}[]

Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-00aa004b2e24}\inprocserver32[]

Queries value: HKCR\clsid\{7c857801-7381-11cf-884d-

00aa004b2e24}\inprocserver32[threadingmodel]

Queries value: HKCR\interface\{d4781cd6-e5d3-44df-ad94-930efe48a887}\proxystubclsid32[] Queries value: HKCR\interface\{9556dc99-828c-11cf-a37e-00aa003240c7}\proxystubclsid32[]

Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}[]

Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprocserver32[inprocserver32]

Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-ce99a996d9ea}\inprocserver32[]

Queries value: HKCR\clsid\{d68af00a-29cb-43fa-8504-

ce99a996d9ea}\inprocserver32[threadingmodel]

 $Queries \ value: \\ \qquad \qquad \text{HKLM} \\ \text{software} \\ \text{microsoft} \\ \text{wbem} \\ \text{cimom}[processid]$

 $Queries \ value: \\ HKLM \ software \ microsoft \ whem \ cimom[enable private object heap]$

 Queries value:
 HKLM\software\microsoft\wbem\cimom[contextlimit]

 Queries value:
 HKLM\software\microsoft\wbem\cimom[objectlimit]

 Queries value:
 HKLM\software\microsoft\wbem\cimom[identifierlimit]

 Queries value:
 HKCR\clsid\{4590f812-1d3a-11d0-891f-00aa004b2e24}[]

Queries value: HKCR\clsid\{4590f812-1d3a-11d0-891f-

00aa004b2e24}\inprocserver32[inprocserver32]

 $Queries\ value: \qquad \qquad \text{HKCR} \\ \text{clsid} \\ \text{4590f812-1d3a-11d0-891f-00aa004b2e24} \\ \text{linprocserver32[]}$

Queries value: HKCR\clsid\{4590f812-1d3a-11d0-891f-

00aa004b2e24}\inprocserver32[threadingmodel]

Queries value: HKLM\software\microsoft\wbem\cimom[enableobjectvalidation]

Queries value: HKCR\interface\{44aca675-e8fc-11d0-a07c-00c04fb68820}\proxystubclsid32[]

Queries value:

 $\label{thm:local-condition} HKLM \label{thm:local-condition} HKLM \label{thm:local-condition} HKLM \label{thm:local-condition} Similar \label{thm:local-condition} HKLM \label{thm:local-condition} HKLM \label{thm:local-condition} Similar \label{thm:local-condition} HKLM \label{thm:local-condition} Similar \label{thm:local-condition} HKLM \label{thm:local-condition} Similar \label{thm:local-condition} HKLM \label{thm:local-condition} HKLM \label{thm:local-condition} Similar \label{thm:local-condition} HKLM \label{thm:local-condition} Similar \label{thm:local-condition} HKLM \label{thm:local-condition} Similar \label{thm:local-condition} HKLM \label{thm:local-condition} Similar \label{thm:local-condition} Similar \label{thm:local-condition} HKLM \label{thm:local-condition} HKLM \label{thm:local-condition} HKLM \label{thm:local-condition} HKLM \label{thm:local-condition} Similar \label{thm:local-condition} Similar \label{thm:local-condition} Similar \label{thm:local-condition} HKLM \label{thm:local-condition} Similar \label{thm:local-condition} Similar \label{thm:local-condition} Similar \label{thm:local-condition} HKLM \label{thm:local-condition} Similar \label{thm:local-condition} HKLM \label{thm:local-condition} Similar \label{thm:lo$

Queries value: HKLM\software\microsoft\windows nt\currentversion\image file execution

options[disablelocaloverride]

Sets/Creates value: HKLM\software\323546aeee592a07b90b[530957d02ada99668870]

Sets/Creates value: HKLM\software\bfuhgx[eay99xa]
Sets/Creates value: HKLM\software\bfuhgx[wp2ccclpw]