

GitHub Gist

Search...


All gists

Back to GitHub

Sign in

Sign up

Instantly share code, notes, and snippets.



GlebSukhodolskiy / autorun_registry_keys.csv

Created 4 years ago

☆ Star 1

🍴 Fork 0

<> Code

🔄 Revisions 1

☆ Stars 1

Embed <script src="https://>

📄

📄

Download ZIP

Autorun Registry Keys

<> autorun_registry_keys.csv

Raw

We can make this file [beautiful and searchable](#) if this error is corrected: No commas found in this CSV file in line 0.

```
1 registry_key
2 \SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\InitialProgram
3 \System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms
4 \System\CurrentControlSet\Control\Session Manager\SetupExecute
5 \System\CurrentControlSet\Control\Session Manager\S0InitialCommand
6 \System\CurrentControlSet\Control\Session Manager\KnownDlls
7 \System\CurrentControlSet\Control\Session Manager\Execute
8 \System\CurrentControlSet\Control\Session Manager\BootExecute
9 \System\CurrentControlSet\Control\Session Manager\AppCertDlls
10 \SYSTEM\CurrentControlSet\Control\SecurityProviders\SecurityProviders
11 \SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell
12 \SYSTEM\CurrentControlSet\Control\Print\Providers
13 \SYSTEM\CurrentControlSet\Control\Print\Monitors
14 \SYSTEM\CurrentControlSet\Control\NetworkProvider\Order
15 \SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages
16 \SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages
17 \System\CurrentControlSet\Control\BootVerificationProgram\ImagePath
18 \SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
19 \SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
20 \SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects
21 \Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
22 \Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
23 \SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler
24 \Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
25 \SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls
26 \Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
27 \Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
28 \SOFTWARE\Wow6432Node\Microsoft\Windows CE Services\AutoStartOnDisconnect
29 \SOFTWARE\Wow6432Node\Microsoft\Windows CE Services\AutoStartOnConnect
30 \Software\Wow6432Node\Microsoft\Office\Word\Addins
31 \Software\Wow6432Node\Microsoft\Office\PowerPoint\Addins
32 \Software\Wow6432Node\Microsoft\Office\Outlook\Addins
33 \Software\Wow6432Node\Microsoft\Office\Onenote\Addins
34 \Software\Wow6432Node\Microsoft\Office\Excel\Addins
35 \Software\Wow6432Node\Microsoft\Office\Access\Addins
36 \Software\Wow6432Node\Microsoft\Internet Explorer\Toolbar
37 \Software\Wow6432Node\Microsoft\Internet Explorer\Extensions
38 \Software\Wow6432Node\Microsoft\Internet Explorer\Explorer Bars
39 \Software\Wow6432Node\Microsoft\Command Processor\Autorun
40 \SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components
41 \Software\Wow6432Node\Classes\Folder\ShellEx\PropertySheetHandlers
42 \Software\Wow6432Node\Classes\Folder\ShellEx\ExtShellFolderViews
43 \Software\Wow6432Node\Classes\Folder\ShellEx\DragDropHandlers
44 \Software\Wow6432Node\Classes\Folder\ShellEx\ContextMenuHandlers
45 \Software\Wow6432Node\Classes\Folder\Shellex\ColumnHandlers
46 \Software\Wow6432Node\Classes\Drive\ShellEx\ContextMenuHandlers
47 \Software\Wow6432Node\Classes\Directory\Shellex\PropertySheetHandlers
48 \Software\Wow6432Node\Classes\Directory\Shellex\DragDropHandlers
49 \Software\Wow6432Node\Classes\Directory\Shellex\CopyHookHandlers
50 \Software\Wow6432Node\Classes\Directory\ShellEx\ContextMenuHandlers
51 \Software\Wow6432Node\Classes\Directory\Background\ShellEx\ContextMenuHandlers
52 \Software\Wow6432Node\Classes\CLSID\{AC757296-3522-4E11-9862-C17BE5A1767E}\Instance
53 \Software\Wow6432Node\Classes\CLSID\{ABE3B9A4-257D-4B97-BD1A-294AF496222E}\Instance
```

```
54 \Software\Wow6432Node\Classes\CLSID\{7ED96837-96F0-4812-B211-F13C24117ED3}\Instance
55 \Software\Wow6432Node\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance
56 \Software\Wow6432Node\Classes\AllFileSystemObjects\ShellEx\PropertySheetHandlers
57 \Software\Wow6432Node\Classes\AllFileSystemObjects\ShellEx\DragDropHandlers
58 \Software\Wow6432Node\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers
59 \Software\Wow6432Node\Classes\*\ShellEx\PropertySheetHandlers
60 \Software\Wow6432Node\Classes\*\ShellEx\ContextMenuHandlers
61 \Software\Policies\Microsoft\Windows\System\Scripts\Startup
62 \Software\Policies\Microsoft\Windows\System\Scripts\Shutdown
63 \Software\Policies\Microsoft\Windows\System\Scripts\Logon
64 \Software\Policies\Microsoft\Windows\System\Scripts\Logoff
65 \SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
66 \SOFTWARE\Microsoft\Windows\CurrentVersion\Run
67 \Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell
68 \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
69 \Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup
70 \Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Shutdown
71 \Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logon
72 \Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logoff
73 \SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects
74 \Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
75 \Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
76 \SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler
77 \Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
78 \SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers
79 \SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers
80 \SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters
81 \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet
82 \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
83 \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Taskman
84 \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
85 \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GpExtensions
86 \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup
87 \Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells
88 \Software\Microsoft\Windows NT\CurrentVersion\Windows\IconServiceLib
89 \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls
90 \Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
91 \SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers
92 \Software\Microsoft\Windows NT\CurrentVersion\Drivers32
93 \SOFTWARE\Microsoft\Windows CE Services\AutoStartOnDisconnect
94 \SOFTWARE\Microsoft\Windows CE Services\AutoStartOnConnect
95 \Software\Microsoft\Office\Word\Addins
96 \Software\Microsoft\Office\PowerPoint\Addins
97 \Software\Microsoft\Office\Outlook\Addins
98 \Software\Microsoft\Office\Onenote\Addins
99 \Software\Microsoft\Office\Excel\Addins
100 \Software\Microsoft\Office\Access\Addins
101 \SOFTWARE\Microsoft\Office test\Special\Perf
102 \Software\Microsoft\Internet Explorer\Toolbar
103 \Software\Microsoft\Internet Explorer\Extensions
104 \Software\Microsoft\Internet Explorer\Explorer Bars
105 \SYSTEM\Setup\CmdLine
106 \Software\Microsoft\Ctf\LangBarAddin
107 \Software\Microsoft\Command Processor\Autorun
108 \SOFTWARE\Microsoft\Active Setup\Installed Components
109 \SOFTWARE\Classes\Protocols\Handler
110 \SOFTWARE\Classes\Protocols\Filter
111 \SOFTWARE\Classes\Htmlfile\Shell\Open\Command\ (Default)
112 \Software\Classes\Folder\ShellEx\PropertySheetHandlers
113 \Software\Classes\Folder\ShellEx\ExtShellFolderViews
114 \Software\Classes\Folder\ShellEx\DragDropHandlers
115 \Software\Classes\Folder\ShellEx\ContextMenuHandlers
116 \Software\Classes\Folder\Shellex\ColumnHandlers
117 \Software\Classes\Filter
118 \SOFTWARE\Classes\Exefile\Shell\Open\Command\ (Default)
119 \Software\Classes\Drive\ShellEx\ContextMenuHandlers
120 \Software\Classes\Directory\Shellex\PropertySheetHandlers
121 \Software\Classes\Directory\Shellex\DragDropHandlers
122 \Software\Classes\Directory\Shellex\CopyHookHandlers
123 \Software\Classes\Directory\ShellEx\ContextMenuHandlers
124 \Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers
125 \Software\Classes\CLSID\{AC757296-3522-4E11-9862-C17BE5A1767E}\Instance
126 \Software\Classes\CLSID\{ABE3B9A4-257D-4B97-BD1A-294AF496222E}\Instance
127 \Software\Classes\CLSID\{7ED96837-96F0-4812-B211-F13C24117ED3}\Instance
```

```
128 \Software\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance
129 \Software\Classes\AllFileSystemObjects\ShellEx\PropertySheetHandlers
130 \Software\Classes\AllFileSystemObjects\ShellEx\DragDropHandlers
131 \Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers
132 \Software\Classes\*.exe
133 \Software\Classes\*.cmd
134 \Software\Classes\*\ShellEx\PropertySheetHandlers
135 \Software\Classes\*\ShellEx\ContextMenuHandlers
136 \Environment\UserInitMprLogonScript
137 \SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop\Scrnsave.exe
138 \System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries64
139 \System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries
140 \System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64
141 \System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries
142 \Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
143 \Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
144 \Software\Microsoft\Internet Explorer\UrlSearchHooks
145 \SOFTWARE\Microsoft\Internet Explorer\Desktop\Components
146 \Software\Classes\Clsid\{AB8902B4-09CA-4bb6-B78D-A8F59079A8D5}\Inprocserver32
147 \Control Panel\Desktop\Scrnsave.exe
```

[Sign up for free](#) to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

