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.

```
registry_key
\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\InitialProgram
\System\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\StartupPrograms
\System\CurrentControlSet\Control\Session Manager\SetupExecute
\System\CurrentControlSet\Control\Session Manager\S0InitialCommand
\System\CurrentControlSet\Control\Session Manager\KnownDlls
\System\CurrentControlSet\Control\Session Manager\Execute
\System\CurrentControlSet\Control\Session Manager\BootExecute
\System\CurrentControlSet\Control\Session Manager\AppCertDlls
\SYSTEM\CurrentControlSet\Control\SecurityProviders\SecurityProviders
\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell
\SYSTEM\CurrentControlSet\Control\Print\Providers
\SYSTEM\CurrentControlSet\Control\Print\Monitors
\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order
\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages
\SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages
\System\CurrentControlSet\Control\BootVerificationProgram\ImagePath
\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects
\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler
\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls
\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Drivers32
\SOFTWARE\Wow6432Node\Microsoft\Windows CE Services\AutoStartOnDisconnect
\SOFTWARE\Wow6432Node\Microsoft\Windows CE Services\AutoStartOnConnect
\Software\Wow6432Node\Microsoft\Office\Word\Addins
\Software\Wow6432Node\Microsoft\Office\PowerPoint\Addins
\Software\Wow6432Node\Microsoft\Office\Outlook\Addins
\Software\Wow6432Node\Microsoft\Office\Onenote\Addins
\Software\Wow6432Node\Microsoft\Office\Excel\Addins
\Software\Wow6432Node\Microsoft\Office\Access\Addins
\Software\Wow6432Node\Microsoft\Internet Explorer\Toolbar
\Software\Wow6432Node\Microsoft\Internet Explorer\Extensions
\Software\Wow6432Node\Microsoft\Internet Explorer\Explorer Bars
\Software\Wow6432Node\Microsoft\Command Processor\Autorun
\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components
\Software\Wow6432Node\Classes\Folder\ShellEx\PropertySheetHandlers
\Software\Wow6432Node\Classes\Folder\ShellEx\ExtShellFolderViews
\Software\Wow6432Node\Classes\Folder\ShellEx\DragDropHandlers
\Software\Wow6432Node\Classes\Folder\ShellEx\ContextMenuHandlers
\Software\Wow6432Node\Classes\Folder\Shellex\ColumnHandlers
\Software\Wow6432Node\Classes\Drive\ShellEx\ContextMenuHandlers
\Software\Wow6432Node\Classes\Directory\Shellex\PropertySheetHandlers
\Software\Wow6432Node\Classes\Directory\Shellex\DragDropHandlers
\Software\Wow6432Node\Classes\Directory\Shellex\CopyHookHandlers
\Software\Wow6432Node\Classes\Directory\ShellEx\ContextMenuHandlers
\Software\Wow6432Node\Classes\Directory\Background\ShellEx\ContextMenuHandlers
\Software\Wow6432Node\Classes\CLSID\{AC757296-3522-4E11-9862-C17BE5A1767E}\Instance
\Software\Wow6432Node\Classes\CLSID\{ABE3B9A4-257D-4B97-BD1A-294AF496222E}\Instance
```

```
\Software\Wow6432Node\Classes\CLSID\{7ED96837-96F0-4812-B211-F13C24117ED3}\Instance
\Software\Wow6432Node\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance
\Software\Wow6432Node\Classes\AllFileSystemObjects\ShellEx\PropertySheetHandlers
\Software\Wow6432Node\Classes\AllFileSystemObjects\ShellEx\DragDropHandlers
\Software\Wow6432Node\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers
\Software\Wow6432Node\Classes\*\ShellEx\PropertySheetHandlers
\Software\Wow6432Node\Classes\*\ShellEx\ContextMenuHandlers
\Software\Policies\Microsoft\Windows\System\Scripts\Startup
\Software\Policies\Microsoft\Windows\System\Scripts\Shutdown
\Software\Policies\Microsoft\Windows\System\Scripts\Logon
\Software\Policies\Microsoft\Windows\System\Scripts\Logoff
\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad
\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
\Software\Microsoft\Windows\CurrentVersion\Policies\System\Shell
\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup
\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Shutdown
\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logon
\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Logoff
\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjects
\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks
\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler
\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers
\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers
\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Provider Filters
\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet
\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit
\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Taskman
\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell
\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GpExtensions
\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup
\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells
\Software\Microsoft\Windows NT\CurrentVersion\Windows\IconServiceLib
\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls
\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Font Drivers
\Software\Microsoft\Windows NT\CurrentVersion\Drivers32
\SOFTWARE\Microsoft\Windows CE Services\AutoStartOnDisconnect
\SOFTWARE\Microsoft\Windows CE Services\AutoStartOnConnect
\Software\Microsoft\Office\Word\Addins
\Software\Microsoft\Office\PowerPoint\Addins
\Software\Microsoft\Office\Outlook\Addins
\Software\Microsoft\Office\Onenote\Addins
\Software\Microsoft\Office\Excel\Addins
\Software\Microsoft\Office\Access\Addins
\SOFTWARE\Microsoft\Office test\Special\Perf
\Software\Microsoft\Internet Explorer\Toolbar
\Software\Microsoft\Internet Explorer\Extensions
\Software\Microsoft\Internet Explorer\Explorer Bars
\SYSTEM\Setup\CmdLine
\Software\Microsoft\Ctf\LangBarAddin
\Software\Microsoft\Command Processor\Autorun
\SOFTWARE\Microsoft\Active Setup\Installed Components
\SOFTWARE\Classes\Protocols\Handler
\SOFTWARE\Classes\Protocols\Filter
\SOFTWARE\Classes\Htmlfile\Shell\Open\Command\(Default)
\Software\Classes\Folder\ShellEx\PropertySheetHandlers
\Software\Classes\Folder\ShellEx\ExtShellFolderViews
\Software\Classes\Folder\ShellEx\DragDropHandlers
\Software\Classes\Folder\ShellEx\ContextMenuHandlers
\Software\Classes\Folder\Shellex\ColumnHandlers
\Software\Classes\Filter
\SOFTWARE\Classes\Exefile\Shell\Open\Command\(Default)
\Software\Classes\Drive\ShellEx\ContextMenuHandlers
\Software\Classes\Directory\Shellex\PropertySheetHandlers
\Software\Classes\Directory\Shellex\DragDropHandlers
\Software\Classes\Directory\Shellex\CopyHookHandlers
\Software\Classes\Directory\ShellEx\ContextMenuHandlers
\Software\Classes\Directory\Background\ShellEx\ContextMenuHandlers
\Software\Classes\CLSID\{AC757296-3522-4E11-9862-C17BE5A1767E}\Instance
\Software\Classes\CLSID\{ABE3B9A4-257D-4B97-BD1A-294AF496222E}\Instance
\Software\Classes\CLSID\{7ED96837-96F0-4812-B211-F13C24117ED3}\Instance
```

```
\Software\Classes\CLSID\{083863F1-70DE-11d0-BD40-00A0C911CE86}\Instance
\Software\Classes\AllFileSystemObjects\ShellEx\PropertySheetHandlers
\Software\Classes\AllFileSystemObjects\ShellEx\DragDropHandlers
\Software\Classes\AllFileSystemObjects\ShellEx\ContextMenuHandlers
\Software\Classes\.exe
\Software\Classes\.cmd
\Software\Classes\*\ShellEx\PropertySheetHandlers
\Software\Classes\*\ShellEx\ContextMenuHandlers
\Environment\UserInitMprLogonScript
\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop\Scrnsave.exe
\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries64
\System\CurrentControlSet\Services\WinSock2\Parameters\Protocol_Catalog9\Catalog_Entries
\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries64
\System\CurrentControlSet\Services\WinSock2\Parameters\NameSpace_Catalog5\Catalog_Entries
\Software\Microsoft\Windows NT\CurrentVersion\Windows\Run
\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load
\Software\Microsoft\Internet Explorer\UrlSearchHooks
\SOFTWARE\Microsoft\Internet Explorer\Desktop\Components
\Software\Classes\Clsid\{AB8902B4-09CA-4bb6-B78D-A8F59079A8D5}\Inprocserver32
\Control Panel\Desktop\Scrnsave.exe
```