woanware

RegRipperRunner

About

woanware is the name for a set of tools and applications I have written. The majority of the tools/applications are related to networking, network security, application security or digital forensic tasks.

Introduction

RegRipperRunner is to replace the functionality of my RegExtract tool e.g. run plugin, run hive, run folder but using Harlan Carvey's regripper, which means it has the same functionality and plugins as regripper without me having to maintain all of the plugins nor navigate via the command line for the numerous plugins that are implemented for it. By its nature it includes some of the plugin browser (pb.pl) and rr.pl functionality which overlapped with the functionality of RegExtract.

Features

- Run single plugin
- Run multiple plugins
- Run against single hive
- Run against all hives in a folder
- Quickly modify the filter lists

Third Party

- NLog : Logging
- ObjectListView : Data viewing via lists
- Registry: Binary registry hive parser (woanware)
- Regripper: RegRipper (Harlan Carvey/keydet89)
- Utility: Misc functions (woanware)

Usage

Modes

RegExtract has four modes for extracting data; Single Plugin, Multiple Plugins, All Plugins and Filter. The mode can be set using the drop down list located on the main toolbar.

The **Single Plugin** mode will run one plugin against the specified hive(s). The **Multiple Plugins** mode allows the user to select one or more plugins to run against the specified hive(s). The **All Plugins** mode will run all applicable plugins against the specified hive(s). The **Filter** mode allows the user to run a preset list of plugins against the specified hives.

Run Plugin

If the **Single Plugin** mode is selected, then the user can double click on the chosen plugin, which will display the File Open dialog window to allow the selection of the registry hive.

Run Hive

The Run Hive option allows the parsing of a single registry hive. The plugins that run against the hive is dependent on the Mode selected.

- Choose the desired Mode
- Select the plugins or filters as appropriate
- Select the Tools->Run Hive menu, a File Open dialog will be displayed
- Select the appropriate registry file
- Click OK

View Plugin

To view the underlying plugin perl code without leaving the application, simply select the plugin and choose the Plugin context menu item.

Run Folder

The Run Folder option allows the parsing of multiple registry hives in one. The plugins that run against the hives is dependent on the Mode selected.

- Choose the desired Mode
- Select the plugins or filters as appropriate
- Select the Tools->Run Folder menu, the Run Folder window will be displayed
- Enter or select the path containing the registry hives
- Click OK

Filters

Filters are designed to group plugins so that data specific to particular case types or hives can be quickly and easily identified. For example fraud cases could have a Filter defined that extracts document related registry information using plugins that deal with MRU lists.

Filters are simply files without file extensions that are loaded from the regripper plugins directory. Various filter related actions can be utilised via the plugin lists context menu. Note that the context menu is only enabled when the Mode is set to Filter.

The context menu allows the user to perform the following actions:

- add plugins to the filter
- delete plugins from the filter
- create new filters
- refresh the filters

Add Plugins

To add plugins to a filter:

- Select the appropriate filter from the drop down list
- Select the plugins to be added using the CTRL or SHIFT keys
- Choose the Filter->Add context menu option. The plugins will be added to the filter file

Delete Plugins

To delete plugins from a filter:

- Select the appropriate filter from the drop down list
- Select the plugins to be added using the CTRL or SHIFT keys
- Choose the Filter->Delete context menu option. The plugins will be removed from the filter file

Create New Filter

To create a new filter:

- Select the plugins to be added using the CTRL or SHIFT keys
- Choose the Filter->New context menu option. The new filter window will be displayed
- Enter the name for the new filter
- Click the OK button, the new filter file will be created. The application will then load the new filter

Refresh

The Filter->Refresh context menu will reload the filters from the regripper plugins directory. This can be used when a filter file has been manually created and saves the user from closing and reopening the application.

History

v1.0.3

- Modified the Run Folder and autorip functionality to use the `SearchOption.AllDirectories` flag, so that will recurse through all sub directories

v1.0.2

- Incorporated Corey Harrell's auto_rip concept. See the following link for more details: http://journeyintoir.blogspot.co.uk/2013/05/unleashing-autorip.html

v1.0.1

- Updated to clear the output textbox when running in plugin mode
- Added missing code to Run Folder button. Thanks randomaccess3

v1.0.0

- Initial public release