







What's new in 3.0?

Rip.exe usage syntax (excerpt)

- r [hive]Registry hive file to parse
- dCheck to see if the hive is dirty
- gGuess the hive file type
- aAutomatically run hive-specific plugins
- aTAutomatically run hive-specific TLN plugins
- f [profile].....use the profile
- p [plugin].....use the plugin

Using RR Effectively

RegRipper is *NOT* “complete” out of the box

Take what you learn from previous cases, bake those things back into your investigations, as plugins

Effectiveness depends on:

- Goals of your investigation
- Version of the OS
- Apps installed on system, and their versions
- How much you “bake” new findings back into your analysis process

Using RR Effectively

Plugins created/updated from open sources + testing...

Ex: RID hijacking added to samparse.pl plugin

Ex: Check for RegEdit “Favorites” added to applets.pl plugin

Ex: Novel persistence mechanisms

Ex: MiniNt key

Using RR Effectively

There are a lot of plugins, all of which may not make sense or be entirely useful right away.

Create runbooks (profiles still available via rip.exe) based on your analysis **goals**

- USB Devices
- Access to mic & webcam

Get granularity & context by correlating Registry data/metadata with other (file system, WEVTX) data sources (timeline)

Future

- Categories
- MITRE ATT&CK mappings
- Analysis Tips - how the output can be used
- References - most plugins have reference URLs in header; add ref URLs to Analysis Tips

Final Notes

I ask that requests be considered thoughtfully.

Recent update to clear GUI textfield between runs was straightforward - tested & updated quickly.

New/updated plugins - can be done quickly, particularly if sample data is provided.

Requests such as "change output format on all plugins to JSON" - consider forking the project.


