Getting the most out of RegRipper

A love story, beyond the gooey

by Harlan Carvey
Overview

➢ What is “RegRipper”?
➢ Do more than what’s available via the GUI
  ➢ “rip –uP”
➢ Plugins != profiles
➢ Profiles == plugins++
“Mommy, where do plugins come from?”

➢ Write your own – people ACTUALLY do this!
➢ Or just ask for help…turn around is pretty quick
➢ Timeline + viewer >> new plugin
The “All” Plugins

- rlo
- del – can also be used with AmCache.hve
- malware
- null
- sizes
- Limits == none
Profiles

➢ What’s in a profile?
➢ Uh…a list of plugins
Summary

➢ Generate default profiles via “rip –uP”
➢ Custom profiles == documented, repeatable processes
➢ Process:
  ➢ New plugins
  ➢ Update default/custom profiles
  ➢ Go nuts!
Shout-outs!

Micah Jones, Mari DeGrazia, Gabriele Zambelli, M. Godfrey, Mitch Impey, Ali Al-Shemery/@binaryz0ne, Phill Moore, etc.
Questions?

keydet89@yahoo.com

https://github.com/keydet89/RegRipper2.8

http://windowsir.blogspot.com