Windows Incident Response

The Windows Incident Response Blog is dedicated to the myriad information surrounding and inherent to the topics of IR and digital analysis of Windows systems. This blog provides information in support of my books; "Windows Forensic Analysis" (1st thru 4th editions), "Windows Registry Forensics", as well as the book I co-authored with Cory Altheide, "Digital Forensics with Open Source Tools".

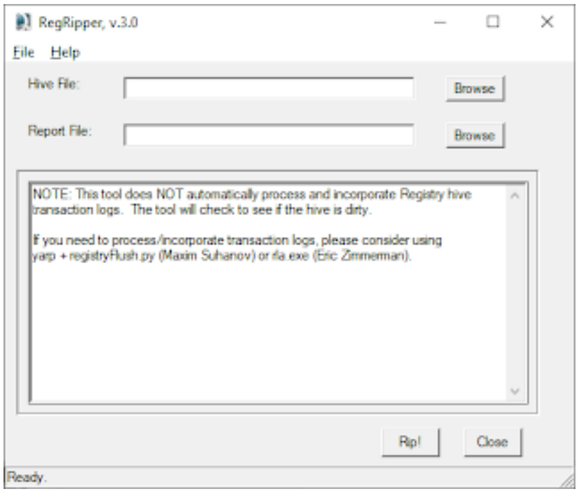
Thursday, May 28, 2020

RegRipper v3.0

I recently released RegRipper v3.0, something I've been working on since Aug, 2019.

I am no longer supporting RegRipper 2.8. I'll leave the repo up for the time being, but I will not be writing plugins to support that version. You can move plugins written for v2.8 to the v3.0 *plugins* folder, and they will work fine. However, due to modifications in the date output format, the reverse is not true.

What's New?



NOTE: This tool does NOT automatically process and incorporate Registry hive transaction logs. The tool will check to see if the hive is dirty.

If you need to process/incorporate transaction logs, please consider using yarp + registryFlush.py (Maxim Suhanov) or rla.exe (Eric Zimmerman).

Ready.

Fig. 1: RegRipper GUI

GUI - The GUI (i.e., rr.exe) no longer makes use of profiles. When you launch the GUI, you'll see what appears in figure 1. Note that you can select the hive, and the output folder for the report, but there is no longer a drop-down for selecting a profile.

Instead, what now happens is that the hive file type is "guessed"/determined, and the tool runs through the entire *plugins* folder to build a list of all plugins that apply to that hive, and then runs them. All of them. There is no longer any need to maintain a profile for use with the GUI. In the end, the idea of profiles seemed to be just too confusing.

The hive file types that RR "knows" are Software, System, SAM, NTUSER.DAT, USRCLASS.DAT, and AmCache.

However, the capability to run individual plugins and profiles still exists, albeit via the command line tool, *rip.exe*. More about that later.

Date Format - the date output format has changed. Phill Moore had asked for this via Twitter back in Feb, and more recently, a Github issue had been submitted via the Autopsy Github site. The issue what was submitted asked for date output format IAW ISO 8601, but what was asked for was not, in fact, compliant with ISO 8601. Rather, what they'd asked for was the RFC 3339 profile. That's very likely much more than you wanted to know, so to be brief, the date output format is now:

```
YYYY-MM-DD HH:MM:SS
```

Pages

Home

Timelines

Books

Malware

FOSS Tools

Subscribe To WindowsIR

Posts

Comments

WindowsIR Blog List

DFIR and Threat Hunting
It's all in the numbers
4 weeks ago

JPCERT/CCブログ 英語版
3 Recommended International Cyber Security Conferences
4 weeks ago

Hacking Exposed Computer Forensics Blog
Daily Blog #701: Magnet Virtual Summit CTF 2020 Results
4 weeks ago

Forensicist
mssql_4n6
2 months ago

Another Forensics Blog
Detecting Lateral Movement with WinSCP

Note the space between the date and time...that's what is NOT compliant with ISO 8601, but it is what was asked for. In those instances where the time stamp is equivalent to UTC, I've added "Z" to the date output format.

Plugin Updates - As part of the process of "fixing" all 386 plugins in the 2.8 distro, a good number of them were updated, modified, consolidated, or simply "whacked". In this case, "whacked" means removed from the main distro, moved to a separate folder, and may be addressed at a later date.

At the moment, the 3.0 distro contains 248 plugins. The easiest way to find something specific in the plugins is to use a hidden MS tool called "findstr". Navigate to the plugins folder and type a command such as:

```
findstr /C:"UseLogonCredential" /i *.pl
```

...or...

```
findstr /C:"pentestlab" /i *.pl
```

If you can't find a plugin that addresses a specific need, then reach out and ask. I recently was provided some information about a key, and some sample data, by a co-worker, and within an hour was able to turn around a fully functional plugin.

RIP - the capabilities of the command line tool have been modified significantly, which you can see from the syntax info below:

```
Rip v.3.0 - CLI RegRipper tool
Rip [-r Reg hive file] [-f profile] [-p plugin] [options]
Parse Windows Registry files, using either a single module, or a profile.

  -r [hive] .........Registry hive file to parse
  -d ................Check to see if the hive is dirty
  -g ................Guess the hive file type
  -a ................Automatically run hive-specific plugins
  -aT ...............Automatically run hive-specific TLN plugins
  -f [profile].......use the profile
  -p [plugin]........use the plugin
  -l ................list all plugins
  -c ................Output plugin list in CSV format (use with -l)
  -s systemname......system name (TLN support)
  -u username........User name (TLN support)
  -uP ...............Update default profiles
  -h.................Help (print this information)

Ex: C:\>rip -r c:\case\system -f system
    C:\>rip -r c:\case\ntuser.dat -p userassist
    C:\>rip -r c:\case\ntuser.dat -a
    C:\>rip -l -c

All output goes to STDOUT; use redirection (ie, > or >>) to output to a file.

copyright 2020 Quantum Analytics Research, LLC
```

Notice the "-a" switch; this replicates what the GUI does, in that it gets the hive file type, then runs through the *plugins* folder and finds all plugins that pertain to that hive type, and then runs them. The "-aT" switch does the same thing, but for the timeline (*_tln.pl) plugins. As with the RR GUI, the hive file types that rip "knows" are Software, System, SAM, NTUSER.DAT, USRCLASS.DAT, and AmCache. However, with *rip.exe*, you can still run the plugins designated for "all" hive types; *rlo.pl*, *null.pl*, *del.pl*, etc., via the command line using the "-p" switch.

3 months ago

1234n6
CyberThreat 2019 Badge Writeup
6 months ago

Digital Forensics Stream
ShellBags & Windows 10 Feature Updates
7 months ago

A Fistful of Dongles
Frustration as Motivation
8 months ago

4n6ir
No Maintenance Artifact Library
11 months ago

Farley Forensics
Hello world!
11 months ago

DFIR on the Mountain
RDP Event Log DFIR
1 year ago

Blog Archive

▼ 2020 (16)
  ► June (2)
  ▼ May (2)
    Tips on Using RegRipper v3.0
    RegRipper v3.0
  ► April (3)
  ► March (2)
  ► February (4)
  ► January (3)
► 2019 (43)
► 2018 (49)
► 2017 (25)
► 2016 (43)
► 2015 (34)
► 2014 (33)
► 2013 (64)
► 2012 (73)
► 2011 (109)

Also, you still have the capability to run profiles via *rip.exe*. This is very useful if you don't want to take a "kitchen sink" approach, but you want to be able to easily run several plugins, such as for a USB playbook.

Caveats
RegRipper is not and never was intended to be an "all knowing" tool. It was intended to be a "good" tool that made people's jobs easier, and the only real way to do that is if analysts provide input. So, rather than saying, "RegRipper doesn't...", why not grab some sample data, attach it to an email and send in a request? I've been pretty good about turning something around within an hour, and more time and more data for testing simply means that the plugin becomes more useful for others, as well.

I haven't seen everything, nor do I know everything. I do not offer myself up as an "expert". This is to say that the available RegRipper plugins are based on either what I've seen or what others have shared with me. For example, I read about Project TajMahal, did some testing, and the *printer_settings.pl* plugin checks to see if the *KeepPrintedJobs* property is enabled. But that doesn't mean the everything pertinent to your case is included in a plugin; if that turns out to be the case, I'm more than happy to assist where I can, and were you allow me to do so.

Posted by H. Carvey at 12:22 PM

Reactions: valuable (1) interesting (0) meh (0)

No comments:

Post a Comment

Links to this post

Create a Link

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

► 2010 (90)
► 2009 (166)
► 2008 (108)
► 2007 (83)
► 2006 (118)
► 2005 (163)
► 2004 (16)