Extending RegRipper

Harlan Carvey
Agenda

- Intro
- Purpose
- Who’s used/using RegRipper??
RegRipper

- Plugin-based approach to extracting/parsing specific Registry data
- Similar to Nessus, but for the Registry
- Write plugins (Perl scripts), engine runs them against the designated hive
- Runs as a GUI, also has a CLI “version”
  - Rip.pl –r NTUSER.DAT –p userassist.pl > ua.txt
RegRipper

![RegRipper Interface](image)
Forensic Scanner

- Extend RegRipper to include more than just the Registry
  - Files (Registry, JumpLists, etc.)
  - Event Logs
  - Scheduled Tasks
  - Prefetch files (XP, Vista/Win7)
  - Etc.

- This is a work-in-progress
Forensic Scanner

FSS, v.1.0

Path: 

Output Dir: 

Profile: 

Scan

Close

Forensic System Scanner v.1.0 opened.
Forensic Scanner

- Run the Forensic Scanner against...
  - Acquired image mounted read-only (ImDisk, FTK Imager, etc.)
  - VMDK added to a VM as an independent, non-persistent hard drive
  - VHD file mounted read-only
    - Convert raw/dd image file using vhdtool.exe
  - Mounted VSC
    - Use CLI to do it repeatedly
  - Live system accessed via F-Response
Forensic Scanner

Use Cases

- HDD imaging and in-processing includes documentation; add a scan, leave analysis to the analyst, as the low-hanging fruit has been identified
- Write plugins based on IoCs, reach out across enterprise with F-Response and scan/triage systems
- On-site analyst sends scanner results and timeline data to off-site analyst to start analysis immediately
- Etc.
Usage

- “Point” scanner at a mounted image
- Run scan; output and log goes to text files
  - Open source: output is configurable (text, XML, etc.)
- Review output
- Retain output and log file with case notes
  - Includes when scan was run/completed, plugins/versions run, info about “system”, etc.
  - Provide both to analyst, so she can analyze
Benefits

- Retention of Intellectual Property/Corporate Knowledge
  - Most scanners are based on this anyway
- Teamwork – *not* all analysts have to have the same experiences
- Establish a career progression
  - Junior team members start w/ acquisitions and scans, provide data to senior analysts, as needed
  - Reading/understanding the plugins helps junior analysts understand what’s going on
Benefits

- Based on scripting language, doesn’t use proprietary API
  - Perl: opendir(), open(), etc.
  - Easily modified/updated (what’s checked, output format, etc.)

Structure

- Basic engine can use platform-dep. GUI solution (Windows GUI, Tk, Qt, etc.)
- Plugins can/should include thorough documentation (comments to code, references, author, etc.)
Plugins

- Scan for high-level indicators
  - List DLL files in C:\Windows dir
  - List PE files in user’s Temp folder

- Scan for specific, low-level indicators
  - Look for specific files (ntshrui.dll, fxsst.dll)
  - List PE sections in imm32.dll
  - Correlate specific Registry entries to files, Event Log entries, etc.
C:\tools>fssc.pl -p G:\Windows -f full -r f:\
Running zeus
Running imm32
Running ntshrui
Running win_dll
Running tasks
Running prefetch
File: G:\Windows\system32\imm32.dll
FileVersion: 5.1.2600.2180
MD5   : 87ca7ce6469577f059297b9d6556d66d

PE Sections:
  .text
  .data
  .rsrc
  .reloc
Questions?

Harlan Carvey

keydet89@yahoo.com