Taking Registry Analysis to the Next Level

Elizabeth Schweinsberg
After Pwn Technologist
How can Registry Analysis help you find the badness on your systems?

- Overview of the favored Malware related Registry keys
- What keys are really being used in the wild?
- Which tools should you use for what?
Malware Related Keys

Run, RunOnce
- SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Services and Drivers
- SYSTEM\CurrentControlSet\Services
- Services Type is 0x10, 0x20, 0x100; Start is 2, 3, or 4 ONLY
- Drivers Type is 0x01 or 0x02; Start is 0 or 1 only??
- Services without “ObjectName” that is set to: LocalSystem, NT AUTHORITY\LocalService, or
- NT AUTHORITY\NetworkService
- Services starting under the Svchost process must have an entry in
  SOFTWARE\Microsoft\Windows NT\CurrentVersion\svchost
Malware Related Keys, cont.

Scheduled Tasks

- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shared Task Scheduler
- SOFTWARE\Classes\CLSID\{GUID}

Browser Helper Objects

- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects

Winlogin and Subkeys

- SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin
- SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin\Notify

How files are run

- SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts
Malware Related Keys, cont.

Application Initialization

- SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs

Actions that happen when cmd starts

- SOFTWARE\Microsoft\Command Processor\Auto Run

Boot Verification

- SYSTEM\CurrentControlSet\Control\BootVerificationProgram

Execute on Boot

- SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute
Where did you get these?

I read books and blogs and stuff

- Windows Forensic Analysis, 2nd Ed by Harlan Carvey
- Windows Registry Forensics by Harlan Carvey
- Footprints Under the Window by Franklin W. Dixon
- Windows Internals, 5th Ed by M Russinovich and D Solomon
- SANS DFIR blog
- Post Humorous Blog
- Windows IR blog
Then how do you know they're useful?

• Good question
  o Run keys are used all the time, but what about the others?

• Who would have a whole bunch of malware *and* have done some analysis about it?
  o AntiVirus companies, perhaps?
  o Repository of malware and technical analyses http://malware.lu
Trawling the Symantec Site


• All of the malware in alpha order by name
• The “Technical Details” page has registry keys listed about 50% of the time as determined by the presence of the string “HKEY”
• 12,000+ writeups, 6100 with registry keys, 47,000+ keys

Do they tell us anything new?
Trawling the Symantec Site - HKCU
Trawling the Symantec Site - HKCU

Not Malware Persistence per se...

Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden
Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\HideFileExt
Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShowSuperHidden
Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoFolderOptions
Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableRegistryTools
Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableTaskMgr
Trawling the Symantec Site - HKCR

- Unique: 31%
- Under 10: 19.2%
- Under 25: 6.9%
- `interface\{CLSID\}`: 24.7%
- `clsid\{CLSID\}`: 3.9%
- `typelib\{CLSID\}`: 9%
- `exefile\shell\open\command`:
- `interface\{CLSID\}\proxystub\clsid\{default\}`:
- `interface\{CLSID\}\nummethods\{default\}`:
- `clsid\{CLSID\}\inprocserver32\threadingmodel`:
- `txtfile\shell\open\command`:
Trawling the Symantec Site - Compare

6360  SOFTWARE\Microsoft\Windows\CurrentVersion\Run
283   SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
2521  SYSTEM\CurrentControlSet\Services
7   SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shared Task Scheduler
365  SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects
423  SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin
110  SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogin\Notify
5    SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\FileExts
20   SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs
3    SOFTWARE\Microsoft\Command Processor\Auto Run
0    SYSTEM\CurrentControlSet\Control\BootVerificationProgram
3    SYSTEM\CurrentControlSet\Control\Session Manager\BootExecute
# Keys to Keep

<table>
<thead>
<tr>
<th>Keep</th>
<th>Downgrade</th>
<th>Add</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Run</td>
<td>• BootVerification</td>
<td>• RunServices</td>
</tr>
<tr>
<td>• Services</td>
<td>• Command Processor\Auto Run</td>
<td>• RunOnce</td>
</tr>
<tr>
<td>• WinLogon</td>
<td>• BootExecute</td>
<td>• Winlogin\Notify</td>
</tr>
<tr>
<td>• Browser Helper Objects</td>
<td>• Explorer\FileExts</td>
<td>• VB and VBA Program Settings</td>
</tr>
<tr>
<td>• AppInit_DLLs</td>
<td>• Shared Task Scheduler</td>
<td>• Internet Settings\Connections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Internet Settings\Zones*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ZoneMap\Domains</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Classes{CLSID}\In ProcServer32</td>
</tr>
</tbody>
</table>
What do I even do with all these keys?
RegRipper

- PERL program with EXE
- Runs a set of plugins on a registry file and outputs the results into a textfile
- Plugins are written in PERL
Registry Decoder - Browsing
Registry Decoder - Plugins

Results for running System Runs against K:\TestReg\software.jen

<table>
<thead>
<tr>
<th>Name</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Tools</td>
<td>C:\Program Files\VMware\VMware Tools\VMwareTray.exe</td>
</tr>
<tr>
<td>VMware User Process</td>
<td>C:\Program Files\VMware\VMware Tools\VMwareUser.exe</td>
</tr>
</tbody>
</table>
Flow Information

GetFile
An efficient file transfer mechanism.

Returns to parent flow:
A jobs_pb2.Path.

Prototype: GetFile(path, pathtype)

Constructor.

This flow uses chunking and hashes to de-duplicate data and send it efficiently.

Args:
path: The directory path to list.
pathtype: Identifies requested path type. Enum from Path protobuf.
pathspec: This flow also accepts all the information in one pathspec.
which is preferred over the path and pathtype definition

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
<th>Next States</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Get information about the file from the client.</td>
<td>Stat, ReadBuffer</td>
</tr>
<tr>
<td>Stat</td>
<td>Fix up the pathspec of the file.</td>
<td>End</td>
</tr>
<tr>
<td>ReadBuffer</td>
<td>Read the buffer and write to the file.</td>
<td>ReadBuffer</td>
</tr>
</tbody>
</table>
```
aff4:/C.a0fdd4bb547cd31b/analysis/RunKeys/System/Run @ 2012-06-18 20:23:57

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>RUNKEYS</td>
<td>keyname: &quot;\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\tvncontrol&quot; 2012-06-16 20:23:57 filepath: &quot;C:\Program Files\TightVNC\tvnserver.exe&quot; -controlservice -slave lastwritten: 1325203845 keyname: &quot;\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\SunJavaUpdateScheduler&quot; filepath: &quot;C:\Program Files\Common Files\Java\Java Update\jusched.exe&quot;&quot; lastwritten: 1325203845</td>
</tr>
<tr>
<td>LABEL</td>
<td>AFF4Index, AFF4Object</td>
</tr>
<tr>
<td>SUBJECT</td>
<td></td>
</tr>
<tr>
<td>+ TYPE</td>
<td>RunKeyCollection</td>
</tr>
</tbody>
</table>
```

**RunKeyCollection**
How do They Rate?

Compare and contrast the 3 tools over 2 samples:

- Testing VM with GRR, RegRipper and RegDecoder
  - Windows 7
  - Extracted the Registry files from the VM using GRR
  - LocalService and NetworkService Users point to the Default Users's NTUser.dat

- nps-2008-jean.E01 with RegRipper and RegDecoder
  - From the Digital Corpora images collection
  - Windows XP
  - Converted E01 file to raw, mounted as loopback and copied Registry files out
  - Could not get the raw image to boot as a VM, so could not test GRR
Testing VM

<table>
<thead>
<tr>
<th>GRR</th>
<th>RegistryDecoder</th>
<th>RegRipper</th>
</tr>
</thead>
<tbody>
<tr>
<td>Found 2 RunOnce keys: 1 in LocalService and 1 in NetworkService</td>
<td>RunOnce keys are listed under the Run key plugin</td>
<td>No plugin detects RunOnce keys</td>
</tr>
<tr>
<td>Found 1 Run keys: 1 in Local Service, 1 in NetworkService, and 2 in System</td>
<td>Found 4 Run keys: 2 in Default and 2 for System</td>
<td>Found 3 Run keys: 1 in Default and 2 in System</td>
</tr>
<tr>
<td>2 BHO</td>
<td>3 BHO, but 2 were repeated</td>
<td></td>
</tr>
<tr>
<td>NSTR in Services</td>
<td>NSTR in Services</td>
<td></td>
</tr>
<tr>
<td>NSTR in WinLogon</td>
<td>NSTR in WinLogon</td>
<td></td>
</tr>
<tr>
<td>GRR</td>
<td>RegistryDecoder</td>
<td>RegRipper</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------------</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>N/A</td>
<td>2 Run Keys for user Jean, 2 Run Keys for the system</td>
<td>2 Run Keys for user Jean, 2 Run Keys for the system</td>
</tr>
<tr>
<td></td>
<td>NSTR in Services</td>
<td>NSTR in Services</td>
</tr>
<tr>
<td></td>
<td>NSTR in WinLogon</td>
<td>NSTR in WinLogon</td>
</tr>
<tr>
<td></td>
<td>1 BHO</td>
<td>1 BHO</td>
</tr>
</tbody>
</table>
# Moving at Scale

<table>
<thead>
<tr>
<th>GRR</th>
<th>Registry Decoder</th>
<th>RegRipper</th>
</tr>
</thead>
<tbody>
<tr>
<td>A work in progress...</td>
<td>Not really built for scale</td>
<td>Once either the image is mounted or the registry files are extracted, write a script to run rip.exe across the files for all desired plugins</td>
</tr>
<tr>
<td>• Add Registry Flows to the initial interrogate flow so it is run every time a system is added</td>
<td></td>
<td>&gt; rip.exe -r RegFile -p PluginModule</td>
</tr>
<tr>
<td>• Use a Python script in the GRR console to iterate over all of the clients enrolled to both run the flow and collect results</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Tool Recap

<table>
<thead>
<tr>
<th>GRR</th>
<th>Registry Decoder</th>
<th>RegRipper</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Registry Flows are quick</td>
<td>+ Great UI&lt;br&gt;+ Best for when you need to explore the registry and do targeted queries&lt;br&gt;+ Written in Python&lt;br&gt;+ Write your own plugins in Python&lt;br&gt;- Cannot add a registry to a case once you've started</td>
<td>+ Active Plugin Developer community&lt;br&gt;+ Can be scripted to run across the registries you've extracted or mounted&lt;br&gt;~ Write your own plugins in PERL</td>
</tr>
</tbody>
</table>
Let's say some registry files fell off a truck...

• The long tail for Run keys is \(~ 50\%\) of the keys

• BUT the number of distinct values for Run keys is small
  
  o 86\% of values had the same data (e.g. file path) when merely converting to all lowercase and removing usernames
  
  o Further improvements will be found with normalizing for version numbers
Analysis at Scale

- HKU/RunOnce: 17.9%
- HKU/Run: 43%
- HKLM/RunOnce: 5.2%
- HKLM/Run: 34%

Bar chart showing:
- Unique Keys:
  - HKU/RunOnce: 0
  - HKU/Run: 500
  - HKLM/RunOnce: 0
  - HKLM/Run: 250
- Long Tail:
  - HKU/RunOnce: 0
  - HKU/Run: 375
  - HKLM/RunOnce: 0
  - HKLM/Run: 125
Summary Judgement

How can Registry Analysis help you find the badness on your systems?

There are more keys to look at and research...
But a few to probably not worry about

If you aren't using RegRipper and Registry Decoder for your analysis -- start

Normalizing your Run keys will help you know when "it's probably fine"
Acknowledgments

NPS and Simson Garfinkle for the Digital Corpora project and images:
   http://digitalcorpora.org/

The GRR Development Team!
   http://code.google.com/p/grr/

Harlan Carvey for RegRipper

All the RegRipper plugin writers!
   http://regripper.wordpress.com/regripper/
   http://code.google.com/p/winforensicaanalysis/downloads/list
   http://code.google.com/p/regripperplugins/

Digital Forensics Solutions for Registry Decoder
   Andrew Case and Vico Marziale
   http://www.digitalforensicssolutions.com/registrydecoder/
Google IR Road Show

BlackHat
July 25, 2012 in Las Vegas, NV
Morgan Marquis-Boire on CuteCats.exe and the Arab Spring

DFRWS
Sunday, August 5 2012 in Washington, DC
Dr. Michael Cohen on Memory Forensics with Volatility 3 hour Workshop

Open Source Digital Forensics Conference
October 3, 2012 in Chantilly, VA
Cory Altheide on ?? Does it even matter? It'll be hilarious and educational
Darren Bilby on GRR
Dr. Michael Cohen on Volatility
Joachim Metz on Volume Service Snapshot (VSS)