MALWARE ANALYSIS TOOLS
developed by CERT.at

Christian Wojner, CERT.at
License

- ISC License

Copyright (c) Year(s), Company or Person's Name <E-mail address>

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
Crossplatform

- Our tools are available for ...  
  - Windows 32 Bit  
  - Windows 64 Bit  
  - Linux 32 Bit  
  - Linux 64 Bit  
  - (Mac OS, not yet - when it's done)
Bytehist

- Generates byte-usage-histograms (distribution)
- For all types of files
- With a special focus on binary executables in PE-format (Windows).
Bytehist

- PE-Sections!
Densityscout

- Mathematically based on Bytehist
- Computing (all) files of a filesystem location
- Result is a descending ordered list
- Reveals potentially unwanted software

07.10.2012
Minibis

- Automation framework based on virtual machines (since 2009!!)
- Highly flexible and configurable
- Easy automation of behavioral analysis tasks
- It does what YOU want
- Can be used in any kind of scenario
- Used in CERT.at's productive processes
- Too complex to summarize
- Update is about to come soon
ProcDOT

- NEW! (Early alpha, but already stable)
- Visualizes Procmon and PCAP (Windump, Tcpdump) logfiles in one graph using Graphviz
- Even highly complicated situations are easy to understand
- Standalone tool based on a Minibis sub-module
- Interactive
<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thread.</td>
<td>Created during monitoring. Still alive after monitoring.</td>
</tr>
<tr>
<td>Server.</td>
<td>[x] = Order of contact</td>
</tr>
<tr>
<td>Registry-Key.</td>
<td>Or a group of Registry keys in compressed graphs.</td>
</tr>
<tr>
<td>Read/Get/Receive.</td>
<td>Thicker lines indicate the number of log-records.</td>
</tr>
<tr>
<td>Create.</td>
<td>A process or a thread.</td>
</tr>
<tr>
<td>RegValue.</td>
<td>A file/URL that is set as Registry key value.</td>
</tr>
<tr>
<td>File.</td>
<td>With creation/existence unknown set as RegValue. (Might also be an URL.)</td>
</tr>
<tr>
<td>File.</td>
<td>Or a group of specific files in compressed graphs.</td>
</tr>
<tr>
<td>Write/Set/Send.</td>
<td>Thicker lines indicate the number of log-records.</td>
</tr>
<tr>
<td>Injection.</td>
<td>A thread is created in some other process.</td>
</tr>
<tr>
<td>Module.</td>
<td>For a specific process.</td>
</tr>
</tbody>
</table>
ProcDOT

- Searching for strings (here: "explorer.exe") ...
ProcDOT

- Searching for strings (here: "inject") ...
Homepage: http://cert.at

Tools: http://cert.at/downloads/software/ListPage1_en.html

Contact: wojner@cert.at