Visual Malware Analysis

Christian Wojner, CERT.at
Person

- Christian Wojner
- Malware Analysis, Reverse Engineering, Computer Forensics
- CERT.at / GovCERT.gv.at

Publications

- Papers
  - Mass Malware Analysis: A DIY Kit
  - An Analysis of the Skype IMBot Logic and Functionality
  - The WOW-Effect
- Articles
  - HITB Online Mag
  - The Art of DLL Injection
  - Automated Malware Analysis - An Introduction to Minibis
  - HAKIN9 Online Mag
  - Minibis
- Software
  - Minibis
  - Bytehist (REMnux)
  - Densitiescout (REMnux)
  - ProcDOT (REMnux)

Speaker

- FIRST Symposium 2010
- CertVerbund-DE 2010
- Deepsec 2010
- Teliasona 2011
- Joint FIRST/TF-CSIRT Technical Seminar 2012
- CanSecWest 2012
- CertVerbund-DE 2012
- 0ct0b3rf3st 2012
- SANS Forensic Summit Prague 2012
- Deepsec 2012
I had a dream ...

- Malware infections are complex
- Humans are visually oriented
- Pictures tell a 1000 words
- Humans are top in understanding complex pictures
- Goal: Put all aspects of a malware infection in one big picture using the most common of freely available tools
- Goal: Distinguish between good/evil with a glance
- Goal: Gut feeling for an entire situation within minutes
- Goal: Freely available to everyone
Proof of concept
Proof of concept
ProcDOT – The name

- Proc ...
  - Process Monitor (Procmon) from Sysinternals
- DOT ...
  - DOT module of the Graphviz Suite
Behavioral analysis

- Monitoring activities

<table>
<thead>
<tr>
<th>Activity</th>
<th>Procmon</th>
<th>PCAP (Windump, Tcpdump, Wireshark)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filesystem</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Network</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Windows Messages</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Registry</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Process-Management</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Thread-Management</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>
Data-Correlation

PROCMON Data → PROCESSES ← PCAP Data

02.04.2013
Noise (-reduction)

- Relevance: Smart-Following-Algorithms
- Paths
- Compression
  - Registry
  - Files
  - Networktraffic
- Filters
  - Files
  - Registrykeys
  - Servers
  - (Longnames/Shortnames)
- Contents
  - Nodes
  - Edges
LIVE DEMO
Reactions?

- Flowers
- Presents
- Kisses
- Hugs
- Handshakes
- Slaps
- Smalltalks
- Longtalks
- Shortdrinks
- Longdrinks
- Questions
- Feedback

02.04.2013
Website:
http://www.cert.at/downloads/software/procdot_en.html

News:
https://twitter.com/ProcDOT

Forum:
https://groups.google.com/forum/#!forum/procdot

Contact:
team@cert.at