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)
  - Densityscout (REMnux)
  - ProcDOT (REMnux)

Speaker

- FIRST Symposium 2010
- CertVerbund-DE 2010
- Deepsec 2010
- Teliasonera 2011
- Joint FIRST/TF-CSIRT Technical Seminar 2012
- CanSecWest 2012
- CertVerbund-DE 2012
- 0ct0b3rf3st 2012
- SANS Forensic Summit Prague 2012
- Deepsec 2012
- FIRST Symposium 2013
- CertVerbund-DE 2013
- 0ct0b3rf3st 2013
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

PCAP Data

PROCESSES

PROC
Graph (Full)
Graph (Part 2/4)

[5] control.exe (PID: 2136) has thread 2140 create process [6] rundll32.exe (PID: 2156) has thread 2160

create file

[3] wPwrz3y.exe (PID: 2120) has thread 2124

is based on

[4] wPwrz3y.exe (PID: 2128) create process

[4] supportotalreg biz 185.680.51

HTTP

HTTP
Graph (Animation)

animation.mp4
Roadmap

v 1.1
- Bitmap Exporter
- Plugin Engine
- Frame/Realtime-Relations (statusbar, markers for 1 & 5 sec)
- UTF-8 aware
- Session based filters (+ global ones)
- Filter Manager

v 1.2
- PCAP Integration ++
  - Flow-DB
  - Node/Edge related functionalities
  - Node/Edge related "Open in Wireshark"
- Frame Ranges
- Notes & Tags
- Reporting Module

(Community) Plugins like
WHOIS
PDNS
etc.

v 1.3
- Themes
- Native Rendering

v ??
- Support native Procmon log format (RE of .pml)

SANS Forensics Prague 2013
Get in touch ... 

- **Website:**

- **News:**
  - https://twitter.com/ProcDOT

- **Community:**
  - https://groups.google.com/forum/#!forum/procdot

- **Donate:**

- **Contact:**
  - team@cert.at