Visualisierung von Malwareverhalten

14. September 2009
- Spring09 -

Pi1 - Laboratory for Dependable Distributed Systems

UNIVERSITÄT MANNHEIM

Motivation

- CWSandbox.org
- Dynamische Malwareanalyse (API-Hooking)
    - Detaillierter Verhaltensreport (XML)
        - 20 Sections / 121 API-Calls
- Ca. 2000 - 4000 neue Sample pro Tag
- Manuelle Auswertung nicht mehr möglich

Motivation

- Was macht die Malware eigentlich?
  - Netzwerkkommunikation?
  - Operationen auf der Registry / in dem Dateisystem?
  - ...
- Was macht die Malware nicht?
- Highlevel-Report?

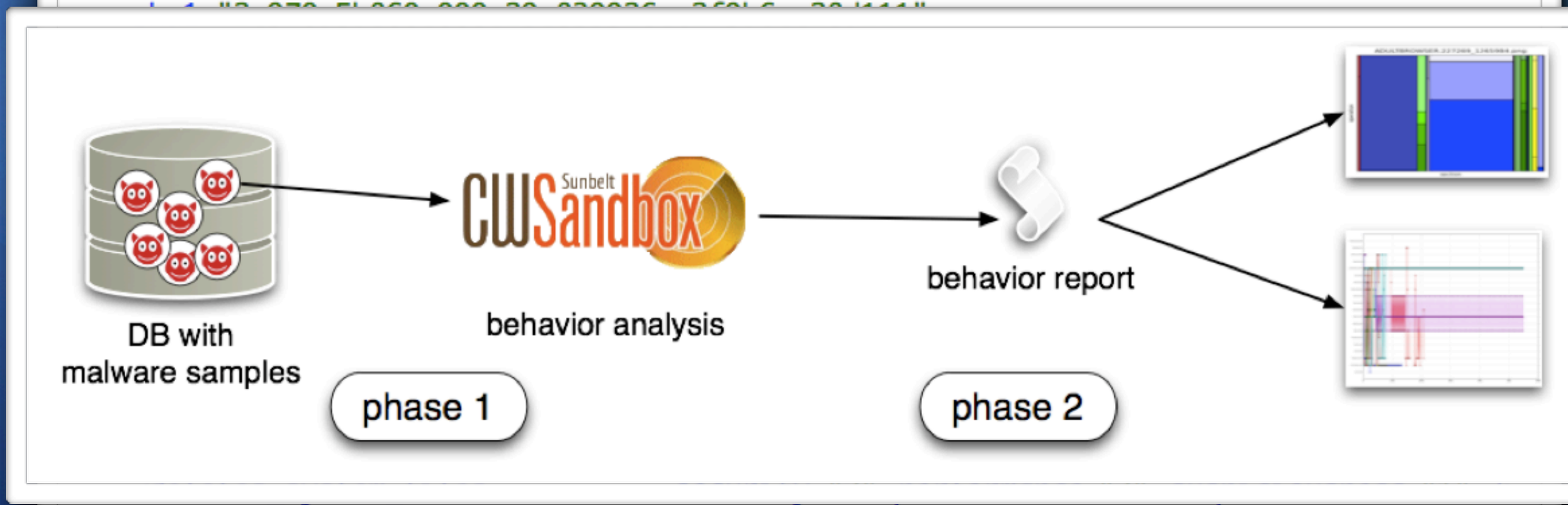
  Welche Samples sind interessant / neu?

Finder File Edit View Go Window Help demo

1265393.xml

```
<open_key key="HKEY_CURRENT_USER\Software\Microsoft\Command Processor"/>
<query_value key="HKEY_CURRENT_USER\Software\Microsoft\Command Processor" value="DisableUNCCheck"/>
<query_value key="HKEY_CURRENT_USER\Software\Microsoft\Command Processor" value="EnableExtensions"/>
<query_value key="HKEY_CURRENT_USER\Software\Microsoft\Command Processor" value="DelayedExpansion"/>
<query_value key="HKEY_CURRENT_USER\Software\Microsoft\Command Processor" value="DefaultColor"/>
<query_value key="HKEY_CURRENT_USER\Software\Microsoft\Command Processor" value="CompletionChar"/>
```

```
<analysis cwsversion="2.1.3" time="10.11.2008 23:23:59"
    file="c:\amun-711284d6174bc9560ab3045785ff5830.exe"
    md5="711284d6174bc9560ab3045785ff5830"
```




```
    <creates_remote_thread                security="2" performance="0" suspiciousness="1" />
</summary>
<scores security="12" performance="5" suspiciousness="9" />
```

```
FILE_LIST_DIRECTORY" shareaccess="FILE_SHARE_READ FILE_SHARE_WRITE" flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="C:\WINDOWS\system32\attrib.exe" srcfile_hash="6be7cccf384b1b05b08b7fc5ae5bc3bb3365cc55"
desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<open_key key="HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers"/>
<open_key key="HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers"/>
<open_key key="HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Custom\attrib.exe"/>
<load_dll filename="C:\WINDOWS\system32\VERSION.dll" successful="1" address="&#x24;77BD0000" end_address="&#x24;77BD8000" size="32768"
```

Line: 1 Column: 1 XML Tab Size: 4

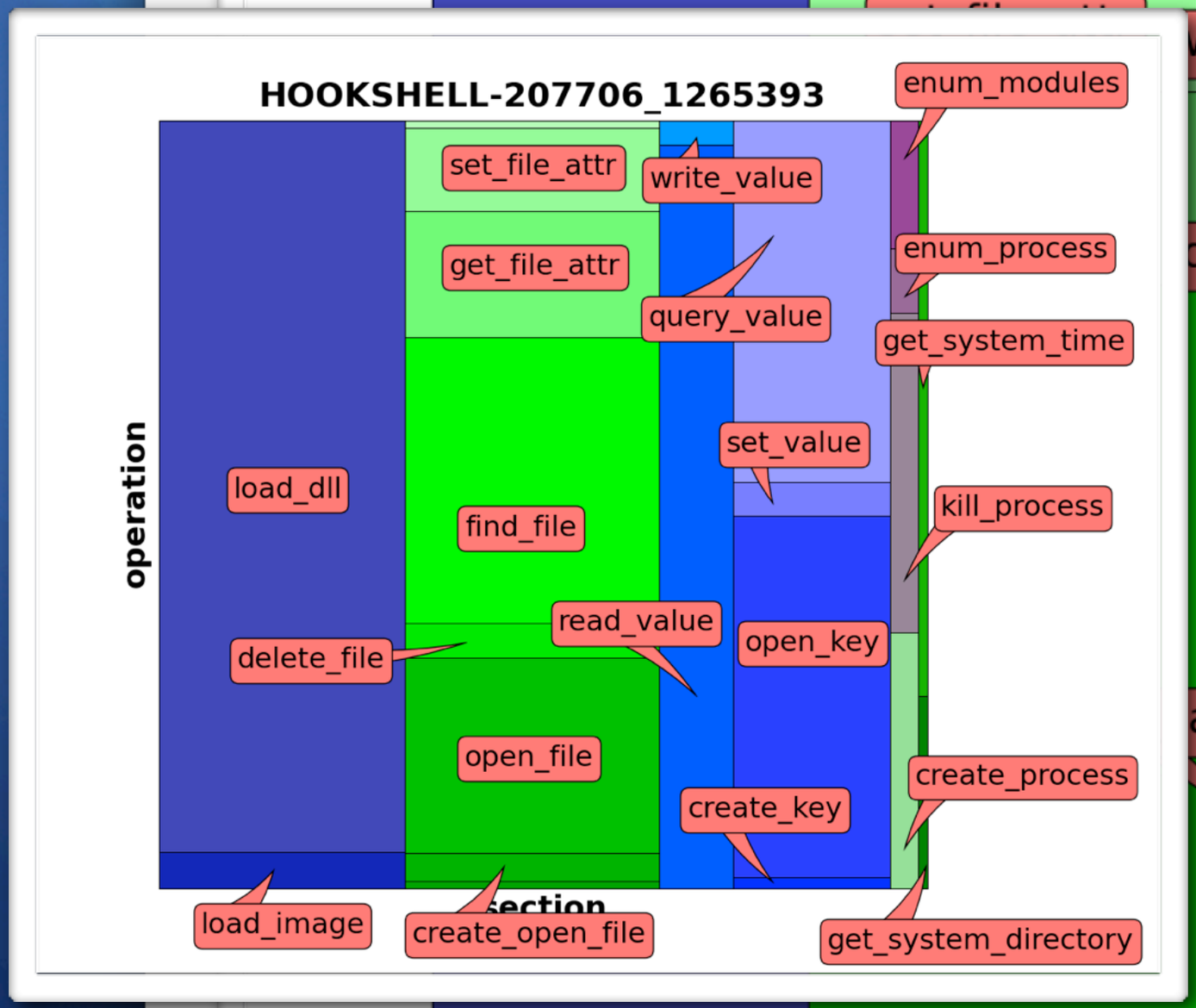
Visualisierung I

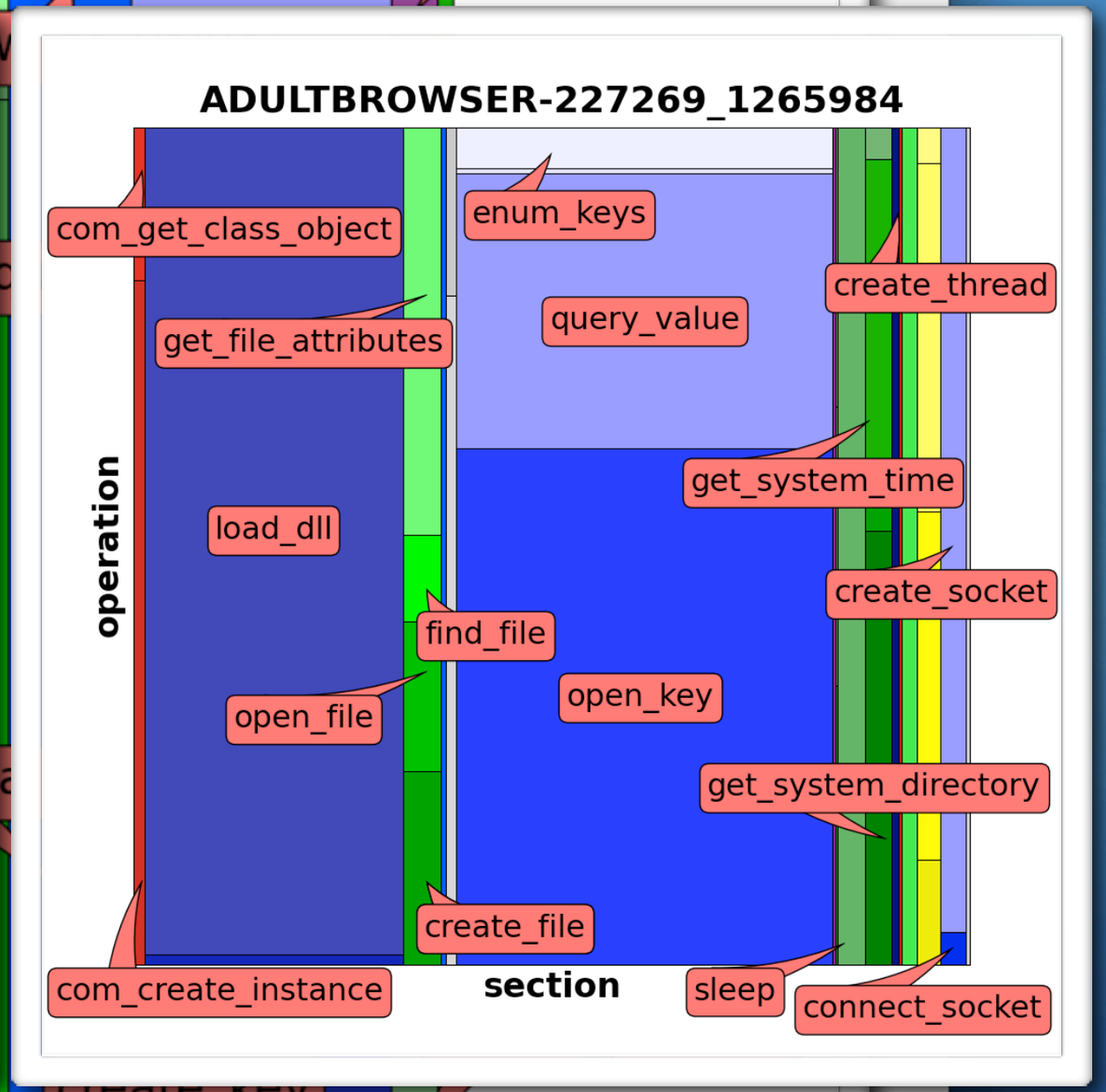
- Treemap
  - Liefert einen schnellen Überblick
  - Codiert ausgeführte Operationen und deren Frequenz
  - Keine Informationen über den Ablauf
- Schnelles Malware-Clustering möglich

Finder File Edit View Go Window Help demo

Treemap

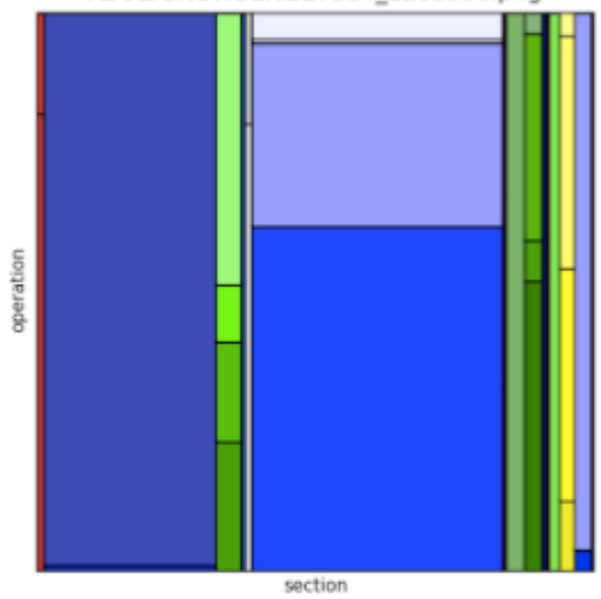
HD



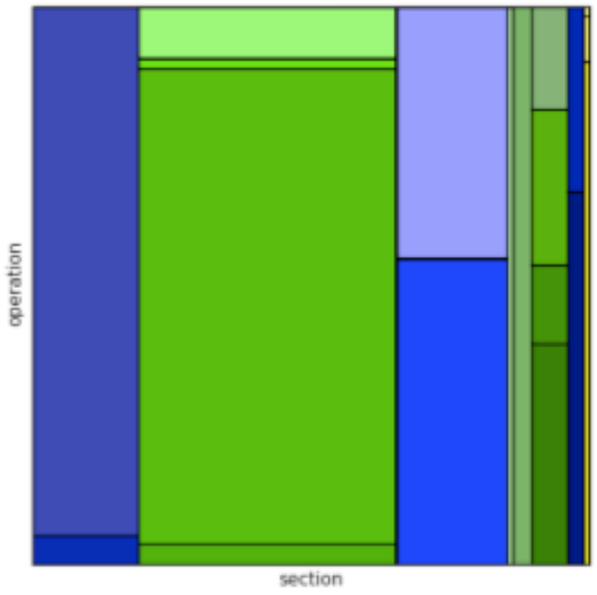


Macintosh HD

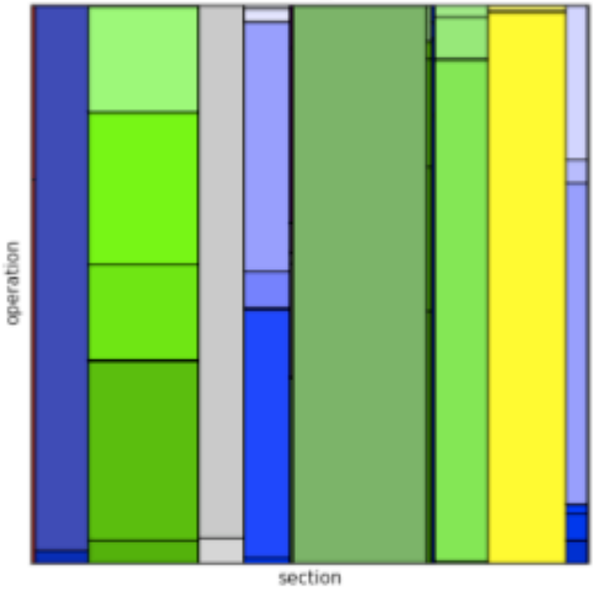
ADULTBROWSER.227364_1265996.png



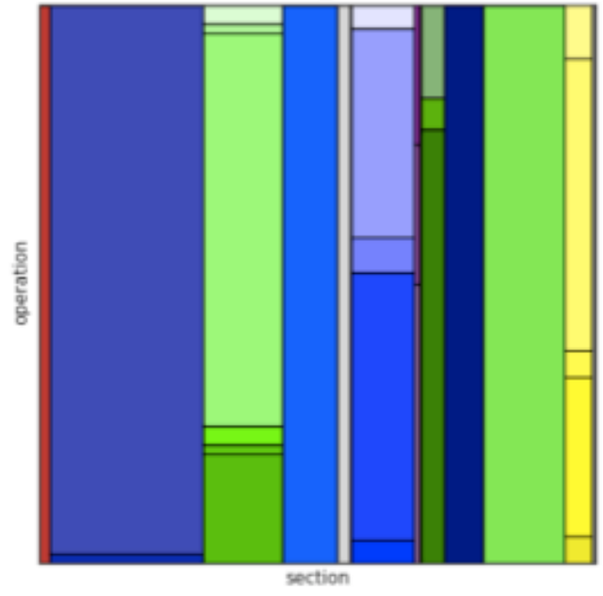
LOOPER.146883_1264370.png



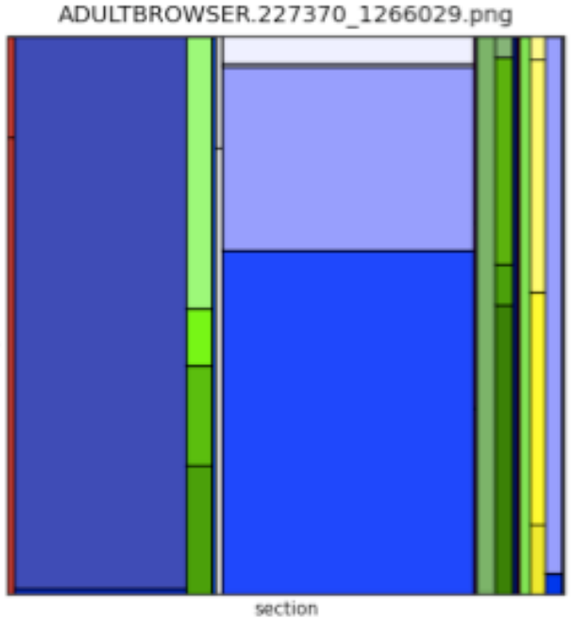
SRAMLER.77234_1264075.png



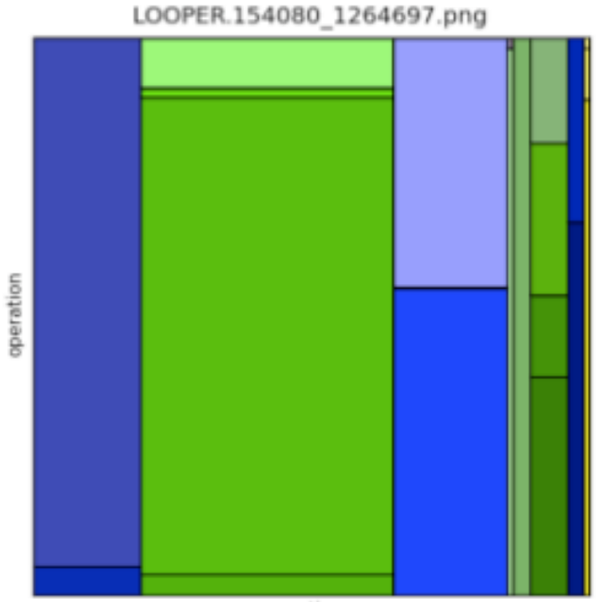
BAGLE.207556_1265374.png



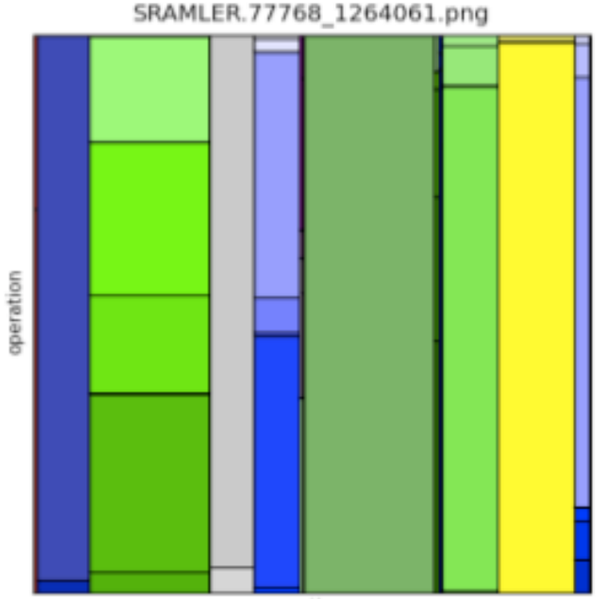
ADULTBROWSER.227370_1266029.png



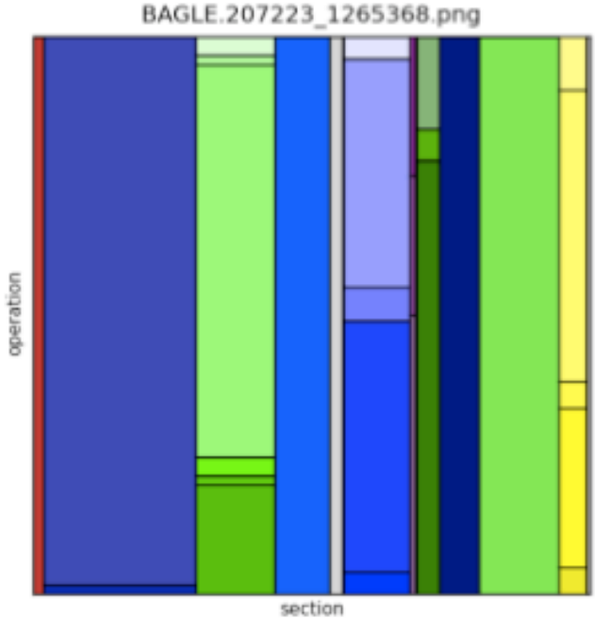
LOOPER.154080_1264697.png



SRAMLER.77768_1264061.png



BAGLE.207223_1265368.png



- Cluster 4 (74 rep, 1 lab)

Visualisierung II

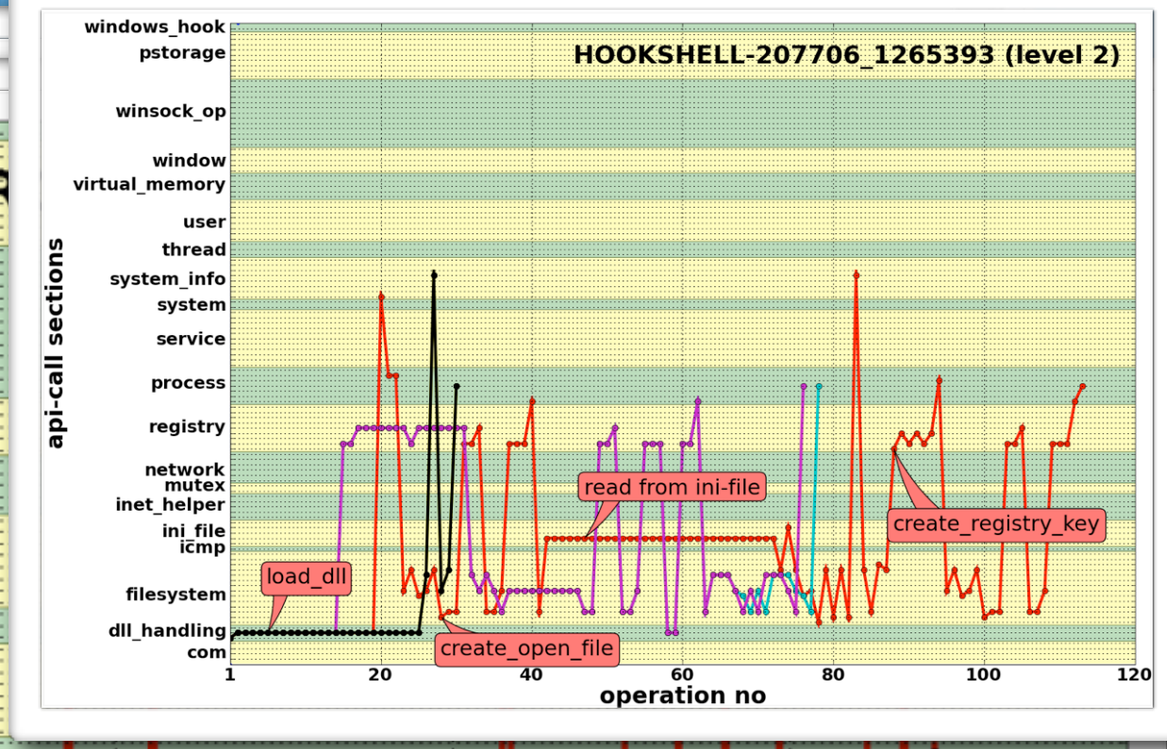
- Threadgraph
  - Zeigt das detaillierte Verhalten aller Threads
  - Alle Operationen werden abgebildet
  - Begrenzung und Zoom nötig (JavaScript)

Finder File Edit View Go Window Help

demo

HOOKSHELL-207706_1265393

enum_modules



operation no

Finder File Edit View Go Window Help demo

Threadgraph

file:///Library/WebServer/Documents/web/threadgraph.html

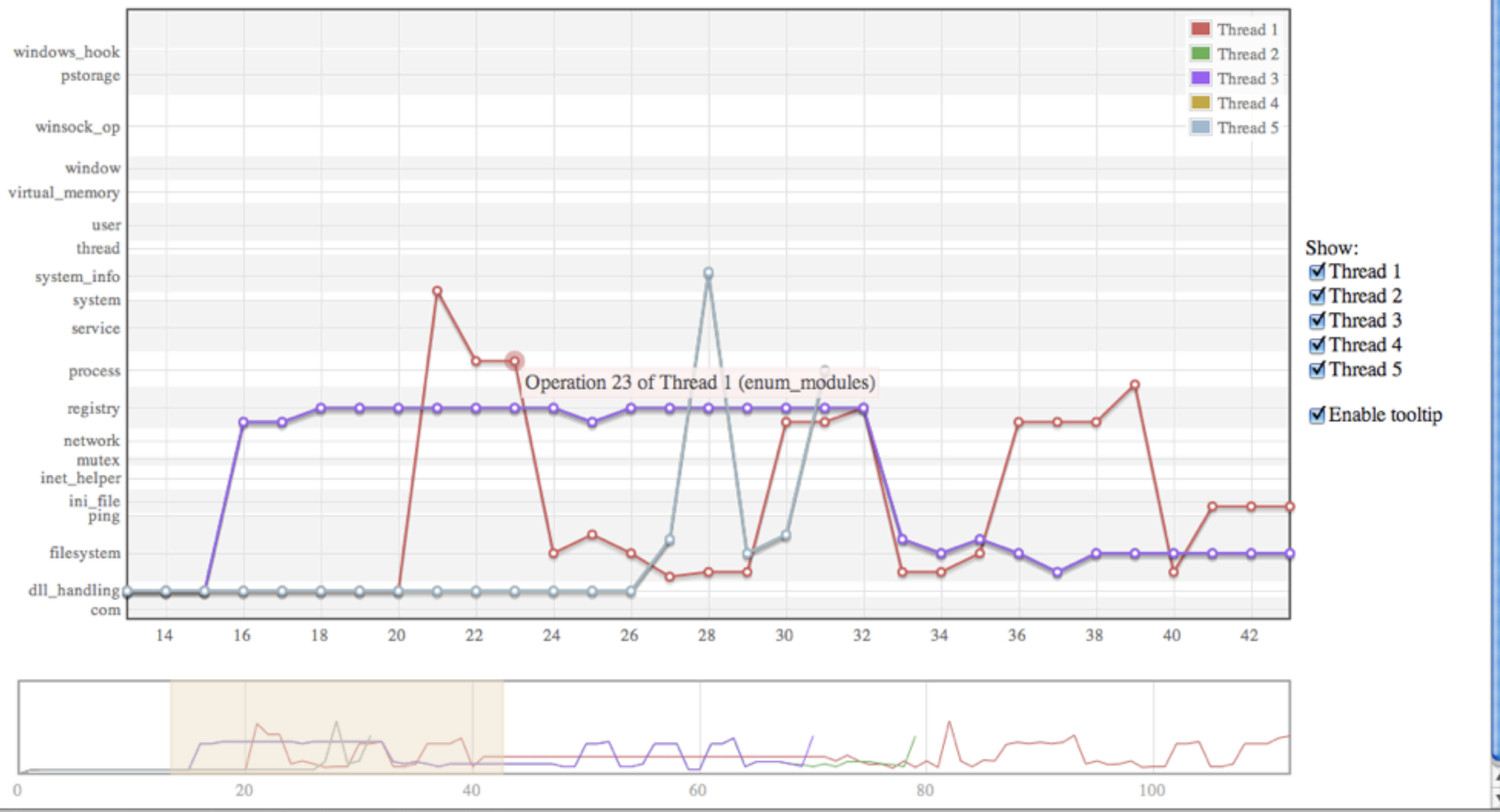
Google

urlaub conferences honeynet flash linux news php private malware python read search sites university iPhone webdesign evaluation

Treemap | Treemap | mal_expt01_single_l1.html | Threadgraph

You clicked Operation 20 of Thread 2.

< query_value value = DelayedExpansion key = HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor />



Show:
- Thread 1
- Thread 2
- Thread 3
- Thread 4
- Thread 5

Enable tooltip

One error in opening the page. For more information, choose Window > Activity.

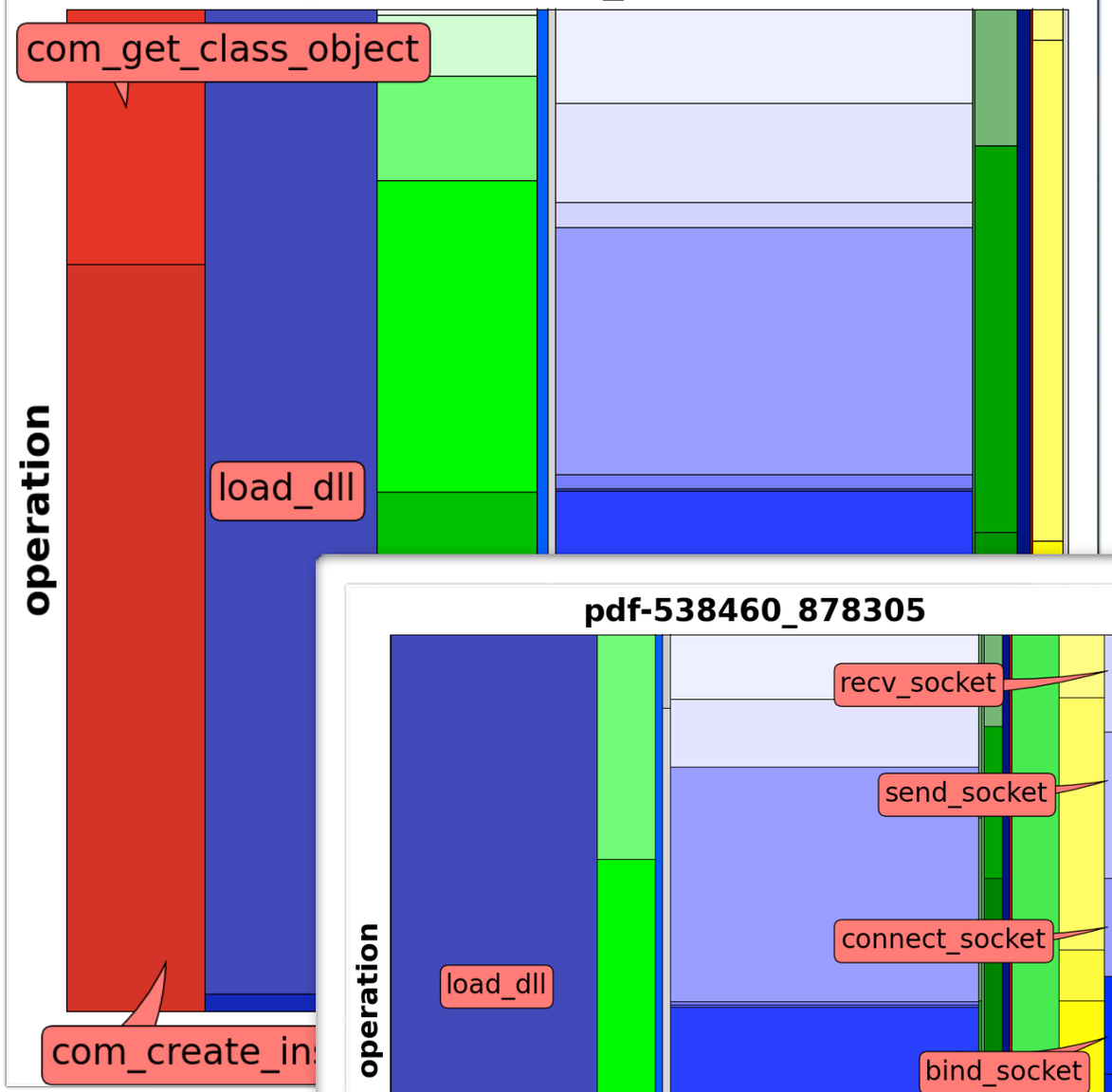
Malicious PDFs

- “CWSandbox analysiert auch Dokumente”
- Test mit 200 gutartigen und 17 (15) infizierten PDFs
- Reports teilen sich in zwei “Treemaps”
- Schadhafte Operationen sind für jeden sofort sichtbar

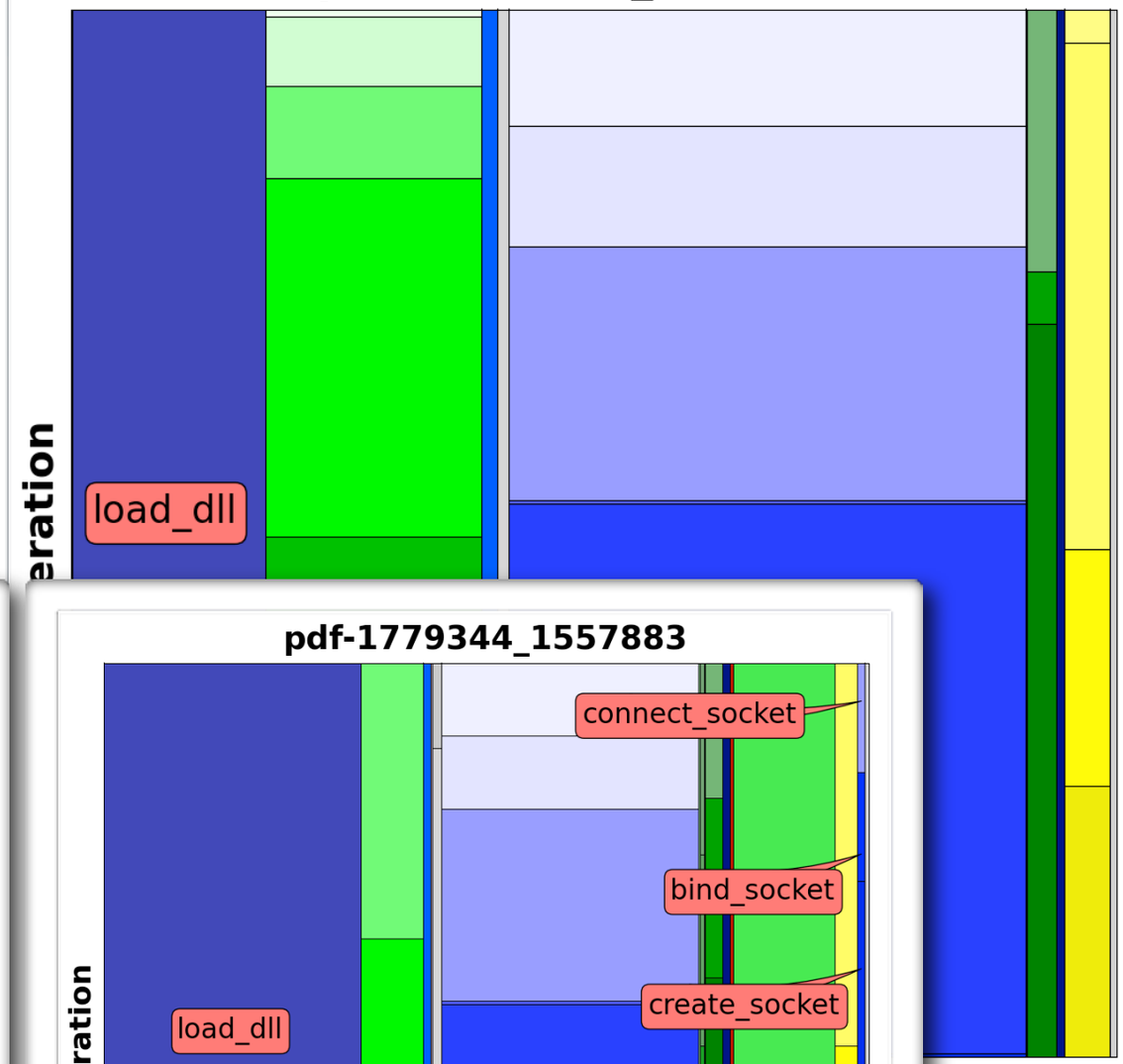
Finder File Edit View Go Window Help demo

Macintosh HD

pdf-1518389_1533525



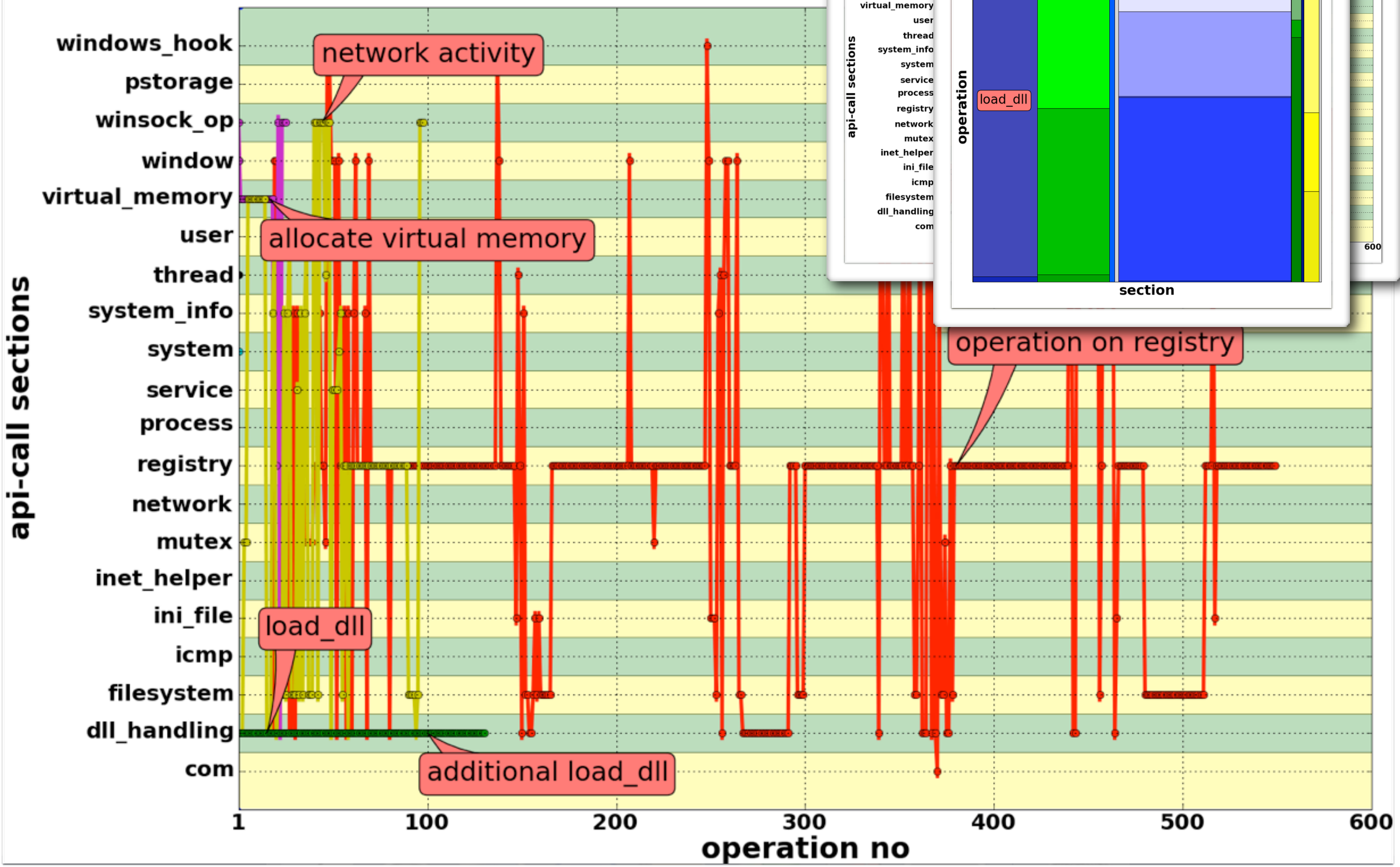
pdf-1518717_1535157



pdf-538460_878305

pdf-1779344_1557883

Finder File Edit View Go Window Help demo



Zusammenfassung

- Bilder sind auf CWSandbox.org verfügbar
  - Statische + JavaScript Versionen
- Feedback ausdrücklich erwünscht

- Studie zu Bilderkennungsalgorithmen
- Weitere Visualisierungsmethoden erarbeiten

Philipp Trinius

http://pi1.informatik.uni-mannheim.de/
trinius@uni-mannheim.de

Pi1 - Laboratory for Dependable Distributed Systems

UNIVERSITÄT MANNHEIM