VisWeek 09

VIS • INFOVIS • VAST

Visual Analysis of Malware Behavior

October 11th, 2009

About Us

- University of Mannheim, Germany

- Laboratory for Dependable Distributed Systems
- Security research:
  - Analysis of malware and spam
  - Honeypots / IT-Forensics

Motivation

- Sandbox Service - *CWSandbox.org*
- Dynamic malware analysis
  - API-Hooking
    - Monitors 121 API-Calls out of 20 sections
    - Detailed Behavior Report (XML)
- Up to 4000 new samples per day
- Manual processing not possible

Motivation

- What are the main Operations?
  - Network activities?
  - Registry access?
  - Filesystem operations?
  - ...
- Which operations do not occur?

Motivation

- What are the main Operations?
  - Network activities?
  - Registry access?
  - Filesystem operations?
  - ...
- Which operations do not occur?

Which samples are of interest?


VisWeek 09
VIS • INFOVIS • VAST

1265393.xml

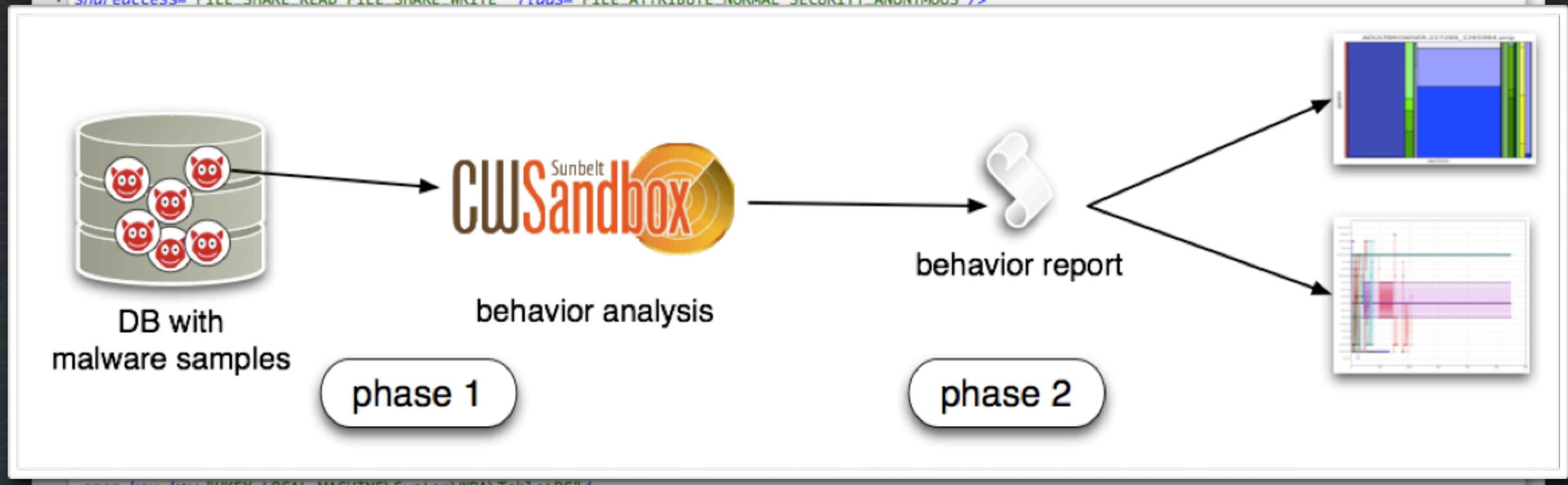
```
<?xml version="1.0"?>
<!-- This analysis was created by CWSandbox (c) CWSE GmbH / Sunbelt Software-->
<analysis cwsversion="2.1.6" time="3/28/2009 10:06:45 PM" file="C:\1265393" md5="a9f6aa1649e6a0f1bfad8a576f0193a0"
sha1="1d13db7f7b57fcc6c715084a20660a464a7aab50" logpath="C:\cwsandbox\log\1265393\run_1\">
<calltree>
<process_call index="1" pid="1164" filename="c:\a9f6aa1649e6a0f1bfad8a576f0193a0" filename_hash="hash_error" starttime="00:00.485"
startreason="AnalysisTarget">
<calltree>
<process_call index="2" pid="1212" filename="C:\DeleteFileDos.bat" filename_hash="hash_error" starttime="00:01.016" startreason="CreateProcess">
<calltree>
<process_call index="4" pid="1244" filename="C:\WINDOWS\system32\attrib.exe attrib c:\a9f6aa1649e6a0f1bfad8a576f0193a0 -r -a -s -h"
filename_hash="6be7cccf384b1b05b08b7fc5ae5bc3bb3365cc55" starttime="00:01.547" startreason="CreateProcess"/>
</calltree>
</process_call>
<process_call index="3" pid="1252" filename="C:\DeleteFileDos.bat" filename_hash="hash_error" starttime="00:01.079" startreason="CreateProcess">
<calltree>
<process_call index="5" pid="1536" filename="C:\WINDOWS\system32\attrib.exe attrib c:\a9f6aa1649e6a0f1bfad8a576f0193a0 -r -a -s -h"
filename_hash="6be7cccf384b1b05b08b7fc5ae5bc3bb3365cc55" starttime="00:01.547" startreason="CreateProcess"/>
</calltree>
</process_call>
</calltree>
</process_call>
</calltree>
<processes>
<process index="1" pid="1164" filename="c:\a9f6aa1649e6a0f1bfad8a576f0193a0" filename_hash="hash_error" filesize="11776"
md5="a9f6aa1649e6a0f1bfad8a576f0193a0" sha1="1d13db7f7b57fcc6c715084a20660a464a7aab50" username="Administrator" parentindex="0" starttime="00:00.485"
terminationtime="00:01.172" startreason="AnalysisTarget" terminationreason="NormalTermination" executionstatus="OK" applicationtype="Win32Application">
<thread tid="1176">
<all_section>
<load_image filename="c:\a9f6aa1649e6a0f1bfad8a576f0193a0" successful="1" address="&#x24;400000" end_address="&#x24;416000" size="90112"
filename_hash="hash_error"/>
<load_dll filename="C:\WINDOWS\system32\ntdll.dll" successful="1" address="&#x24;7C910000" end_address="&#x24;7C9C6000" size="745472"
filename_hash="cc33461f7147042c14d739ba7dc1916e6ccc8139"/>
<load_dll filename="C:\WINDOWS\system32\kernel32.dll" successful="1" address="&#x24;7C800000" end_address="&#x24;7C908000" size="1081344"
filename_hash="e4eb14f7a950a30bc632446a9c9b418837378aac"/>
<load_dll filename="C:\WINDOWS\system32\user32.dll" successful="1" address="&#x24;7E360000" end_address="&#x24;7E3F1000" size="593920"
filename_hash="08fe9ff1fe9b8fd237adedb10d65fb0447b91fe5"/>
<load_dll filename="C:\WINDOWS\system32\GDI32.dll" successful="1" address="&#x24;77EF0000" end_address="&#x24;77F39000" size="299008"
filename_hash="0f37018f672c7635691f7317ade3c5a63904ec96"/>
<load_dll filename="C:\WINDOWS\system32\advapi32.dll" successful="1" address="&#x24;77DA0000" end_address="&#x24;77E4A000" size="696320"
filename_hash="f683eb85535e34c41e5bf5da535d9dcc4aefe8b2"/>
<load_dll filename="C:\WINDOWS\system32\RPCRT4.dll" successful="1" address="&#x24;77E50000" end_address="&#x24;77EE2000" size="598016"
filename_hash="5fa87156724a65171a2cf26c0b0c9aaa04c78d29"/>
<load_dll filename="C:\WINDOWS\system32\Secur32.dll" successful="1" address="&#x24;77FC0000" end_address="&#x24;77FD1000" size="69632"
filename_hash="01c61846bfa5ec977e901ebdb9d0f5372f785010"/>
<load_dll filename="C:\WINDOWS\system32\oleaut32.dll" successful="1" address="&#x24;770F0000" end_address="&#x24;7717B000" size="569344"
filename_hash="3168a173d177f470928b468db777640861dcb32e"/>
<load_dll filename="C:\WINDOWS\system32\msvcrt.dll" successful="1" address="&#x24;77BE0000" end_address="&#x24;77C38000" size="360448"
filename_hash="70d5f97088cc9348bb9d10098af0738a696b96de"/>
```

Line: 1 Column: 1 XML Tab Size: 4

```
<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"/>
<query_value key="HKEY_CURRENT_USER\Software\Microsoft\Command Processor" value="PathCompletionChar"/>
<query_value key="HKEY_CURRENT_USER\Software\Microsoft\Command Processor" value="AutoRun"/>
<get_file_attributes filetype="file" srcfile="C:\" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="C:\" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<get_file_attributes filetype="file" srcfile="C:\" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="C:\DeleteFileDos.bat" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<open_file filetype="file" srcfile="C:\DeleteFileDos.bat" srcfile_hash="hash_error" creationdistribution="OPEN_EXISTING" desiredaccess="FILE_ANY_ACCESS"
shareaccess="FILE_SHARE_READ FILE_SHARE_WRITE" flags="FILE_ATTRIBUTE_NORMAL SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="c:\attrib.&#x2A;" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="c:\attrib" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="C:\WINDOWS\system32\attrib.&#x2A;" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS"
flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="C:\WINDOWS\system32\attrib.COM" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS"
flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="C:\WINDOWS\system32\attrib.EXE" srcfile_hash="6be7cccf384b1b05b08b7fc5ae5bc3bb3365cc55"
desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="c:\attrib.&#x2A;" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="c:\attrib" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="C:\WINDOWS\system32\attrib.&#x2A;" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS"
flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="C:\WINDOWS\system32\attrib.COM" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS"
flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="C:\WINDOWS\system32\attrib.EXE" srcfile_hash="6be7cccf384b1b05b08b7fc5ae5bc3bb3365cc55"
desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<open_file filetype="file" srcfile="C:\WINDOWS\AppPatch\sysmain.sdb" srcfile_hash="891c202c43233e98daa8cdfa1b1272467dd09696"
creationdistribution="OPEN_EXISTING" desiredaccess="FILE_ANY_ACCESS FILE_READ_ATTRIBUTES" shareaccess="FILE_SHARE_READ" flags="FILE_ATTRIBUTE_NORMAL
SECURITY_ANONYMOUS"/>
<open_file filetype="file" srcfile="C:\WINDOWS\AppPatch\systest.sdb" srcfile_hash="hash_error" creationdistribution="OPEN_EXISTING"
desiredaccess="FILE_ANY_ACCESS FILE_READ_ATTRIBUTES" shareaccess="FILE_SHARE_READ" flags="FILE_ATTRIBUTE_NORMAL SECURITY_ANONYMOUS"/>
<open_key key="HKEY_LOCAL_MACHINE\System\WPA\TabletPC"/>
<open_key key="HKEY_LOCAL_MACHINE\SYSTEM\WPA\MediaCenter"/>
<query_value key="HKEY_LOCAL_MACHINE\SYSTEM\WPA\MediaCenter" value="Installed"/>
<open_file filetype="file" srcfile="\Device\NamedPipe\ShimViewer" srcfile_hash="hash_error" creationdistribution="OPEN_EXISTING"
desiredaccess="FILE_ANY_ACCESS FILE_WRITE_ACCESS FILE_WRITE_DATA FILE_ADD_FILE FILE_ADD_SUBDIRECTORY FILE_APPEND_DATA FILE_CREATE_PIPE_INSTANCE
FILE_WRITE_EA FILE_WRITE_ATTRIBUTES" flags="FILE_ATTRIBUTE_NORMAL SECURITY_ANONYMOUS"/>
<open_file filetype="file" srcfile="C:\WINDOWS\system32\" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS FILE_READ_ACCESS FILE_READ_DATA
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"
```

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"/>
<query_value key="HKEY_CURRENT_USER\Software\Microsoft\Command Processor" value="PathCompletionChar"/>
<query_value key="HKEY_CURRENT_USER\Software\Microsoft\Command Processor" value="AutoRun"/>
<get_file_attributes filetype="file" srcfile="C:\" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="C:\" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<get_file_attributes filetype="file" srcfile="C:\" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<find_file filetype="file" srcfile="C:\DeleteFileDos.bat" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS" flags="SECURITY_ANONYMOUS"/>
<open_file filetype="file" srcfile="C:\DeleteFileDos.bat" srcfile_hash="hash_error" creationdistribution="OPEN_EXISTING" desiredaccess="FILE_ANY_ACCESS"
shareaccess="FILE_SHARE_READ FILE_SHARE_WRITE" flags="FILE_ATTRIBUTE_NORMAL SECURITY_ANONYMOUS"/>
```




```
<open_key key="HKEY_LOCAL_MACHINE\System\WPA\TabletPC"/>
<open_key key="HKEY_LOCAL_MACHINE\SYSTEM\WPA\MediaCenter"/>
<query_value key="HKEY_LOCAL_MACHINE\SYSTEM\WPA\MediaCenter" value="Installed"/>
<open_file filetype="file" srcfile="\Device\NamedPipe\ShimViewer" srcfile_hash="hash_error" creationdistribution="OPEN_EXISTING"
desiredaccess="FILE_ANY_ACCESS FILE_WRITE_ACCESS FILE_WRITE_DATA FILE_ADD_FILE FILE_ADD_SUBDIRECTORY FILE_APPEND_DATA FILE_CREATE_PIPE_INSTANCE
FILE_WRITE_EA FILE_WRITE_ATTRIBUTES" flags="FILE_ATTRIBUTE_NORMAL SECURITY_ANONYMOUS"/>
<open_file filetype="file" srcfile="C:\WINDOWS\system32\" srcfile_hash="hash_error" desiredaccess="FILE_ANY_ACCESS FILE_READ_ACCESS FILE_READ_DATA
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

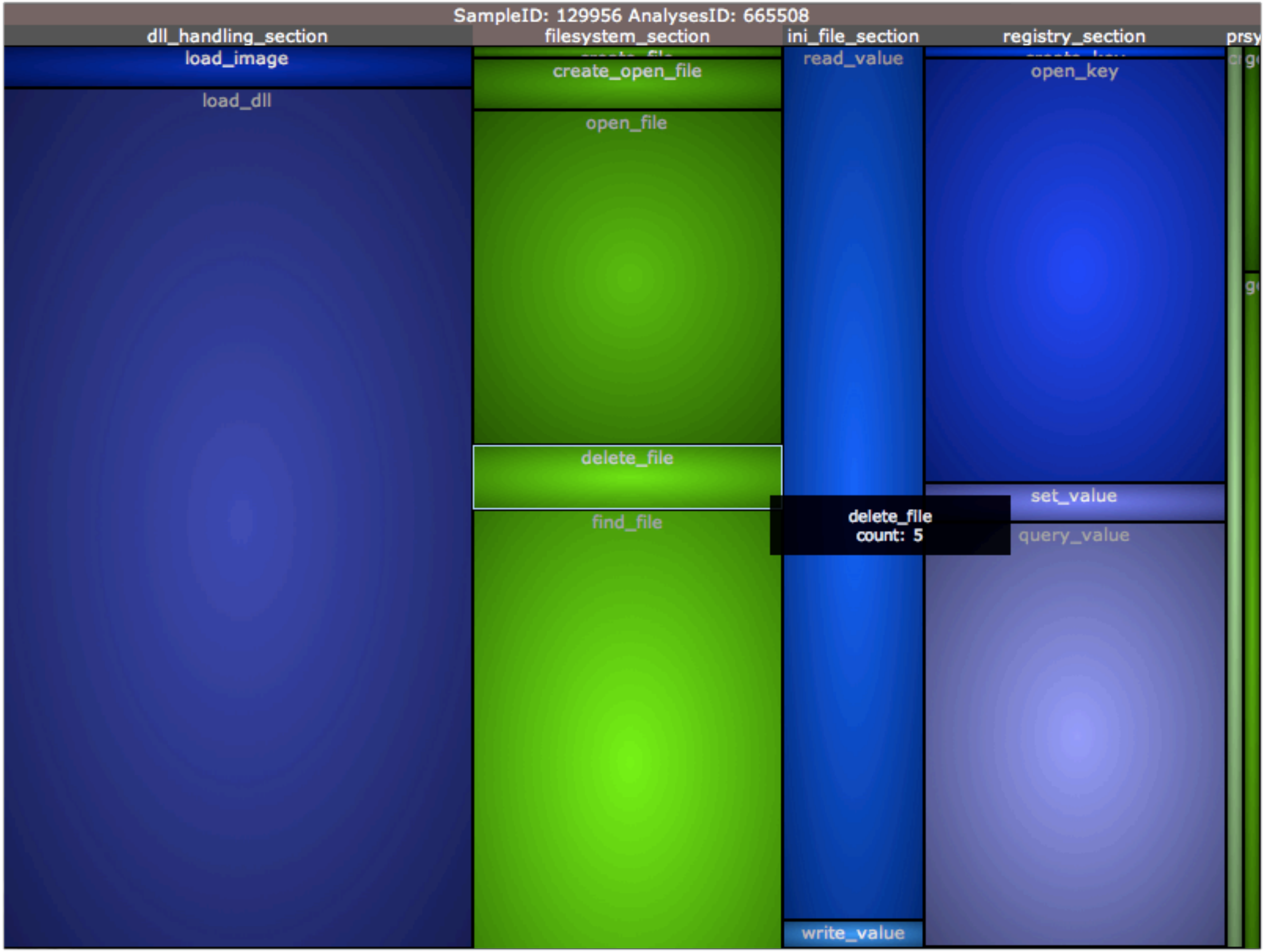
Visualization

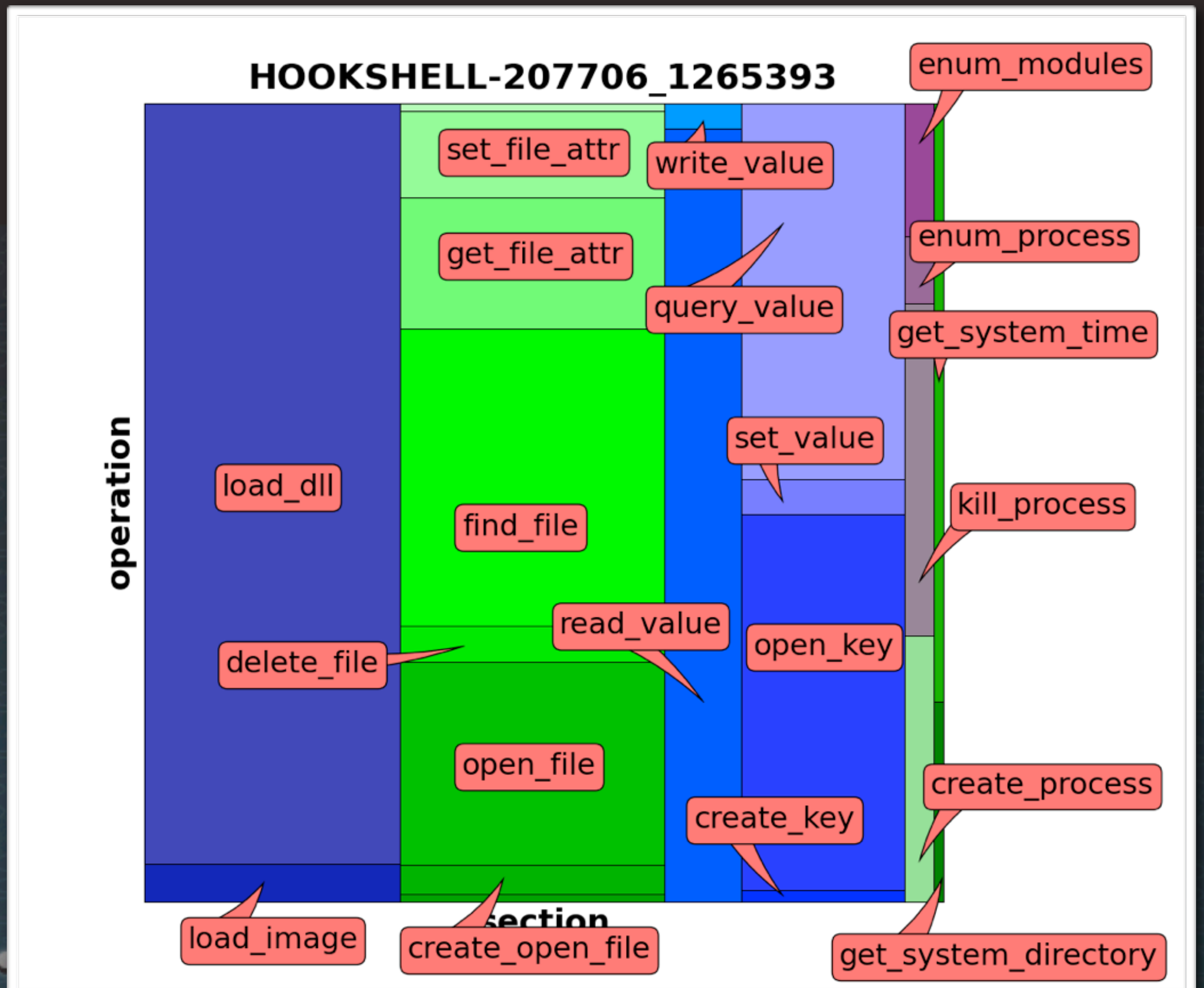
- CWSandbox report is “too” detailed
- Use visualization for abstraction
  - Simple to create
  - Comprehensible
- Treemaps and Threadgraphs
- Static version (Python, matplotlib)
- Dynamic version using JavaScript (flot, Jit)

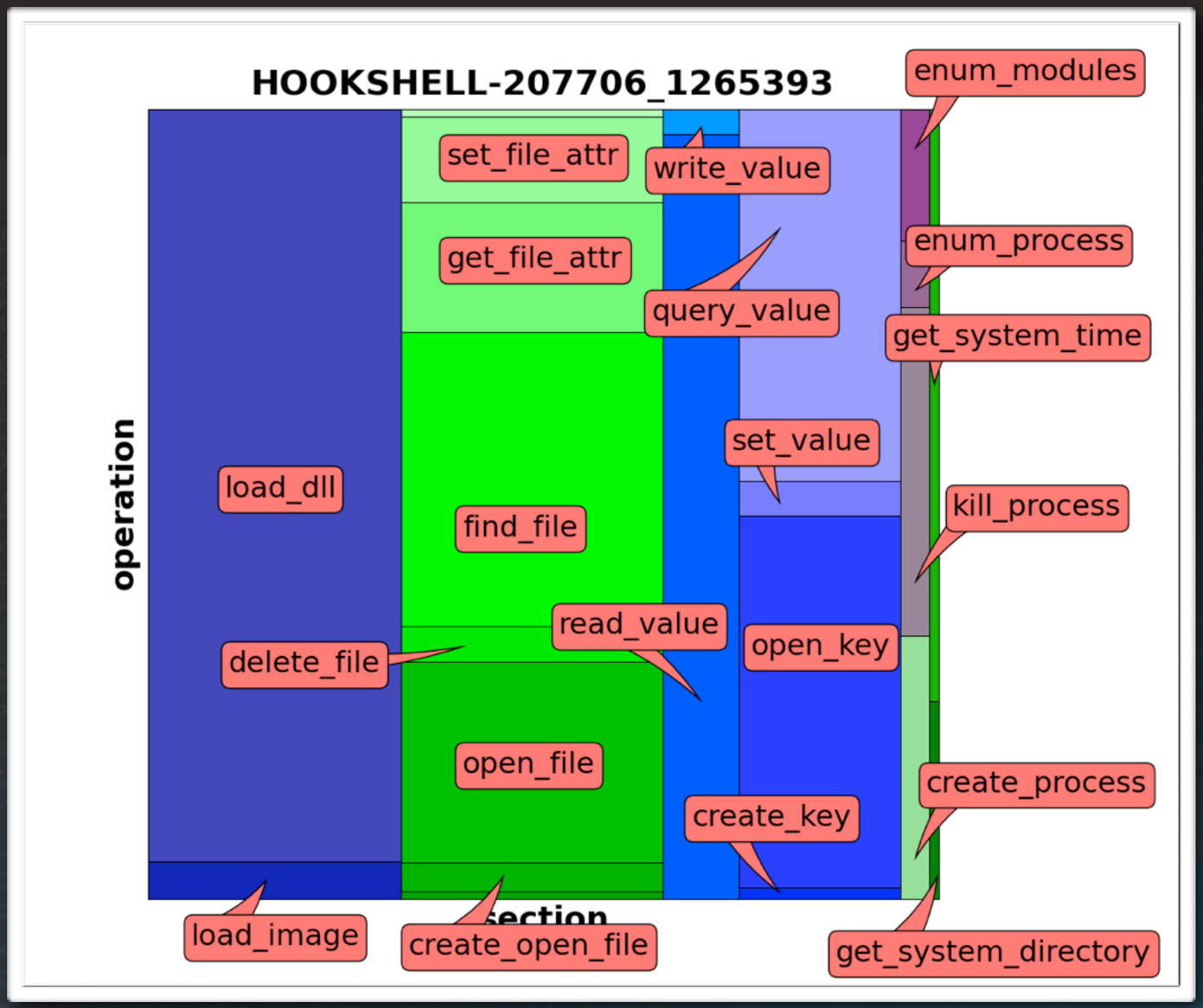
Treemaps

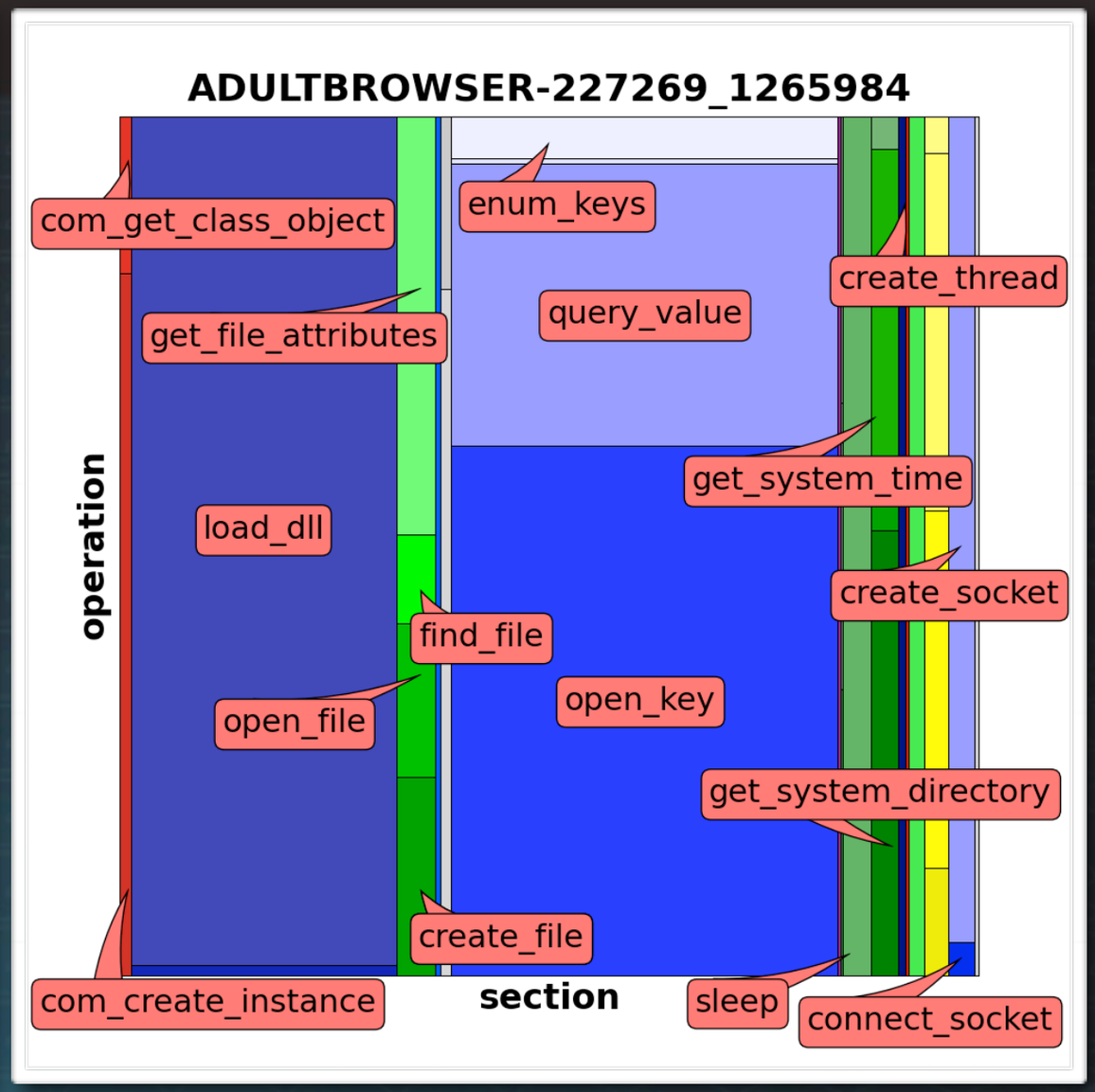
- Quick overview
- Displays the distribution of all operations
- No information about the sequence of operations
- Use case: Malware clustering


VisWeek 09
VIS • INFOVIS • VAST

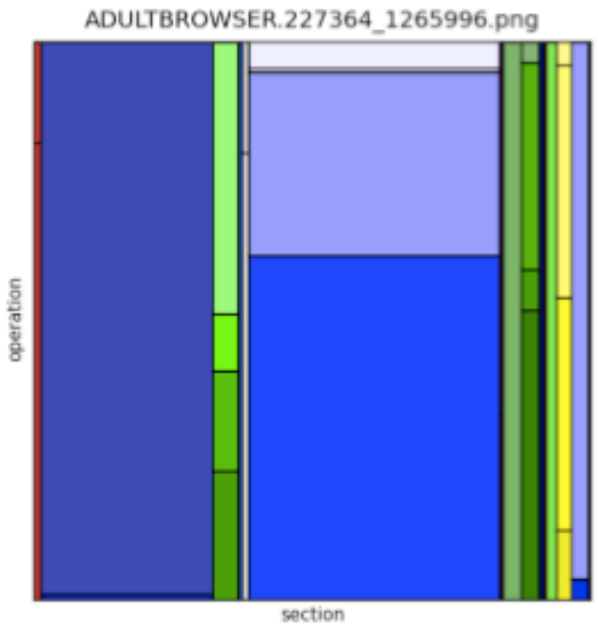


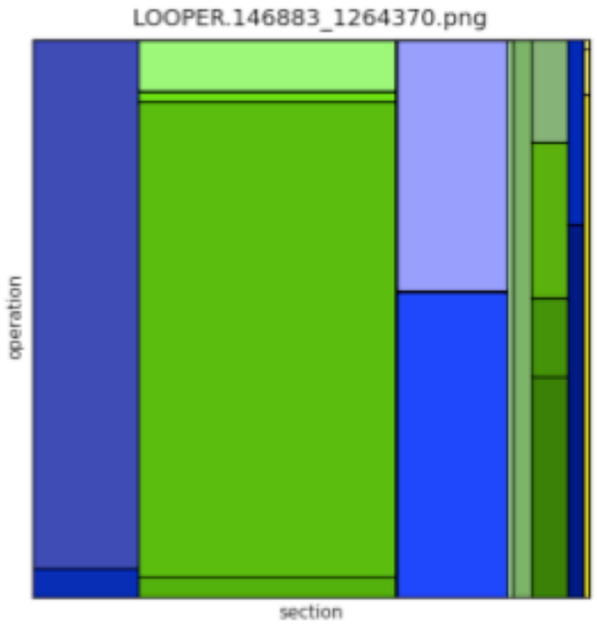

HOOKSHELL-207706_1265393
operation
section
load_dll
set_file_attr
get_file_attr
find_file
delete_file
open_file
load_image
create_open_file
write_value
query_value
read_value
set_value
open_key
create_key
enum_modules
enum_process
get_system_time
kill_process
create_process
get_system_directory

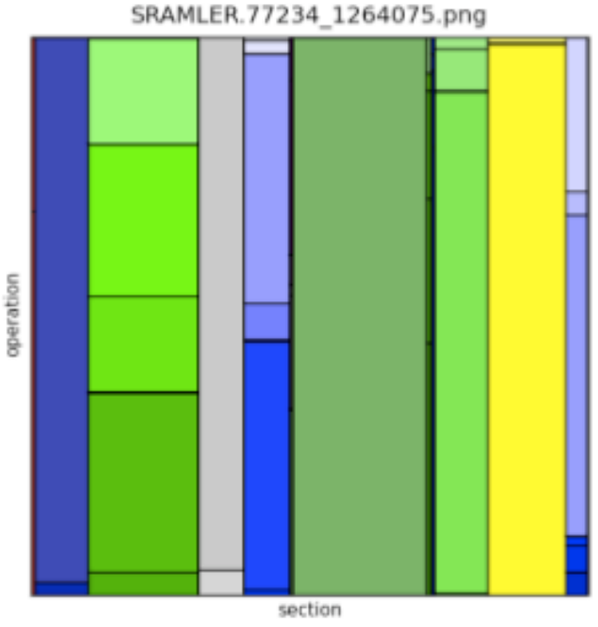


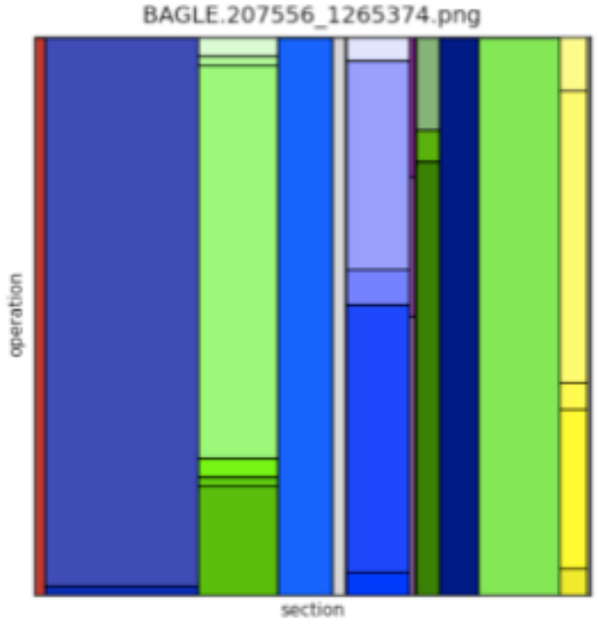


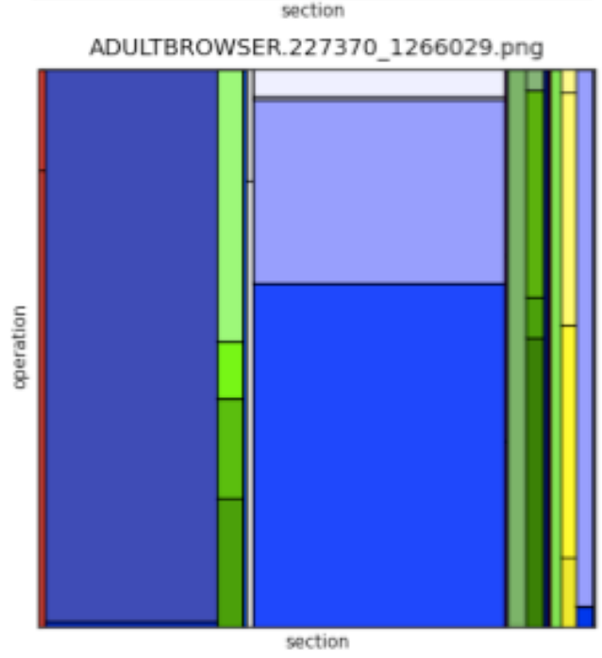

VisWeek 09
VIS • INFOVIS • VAST

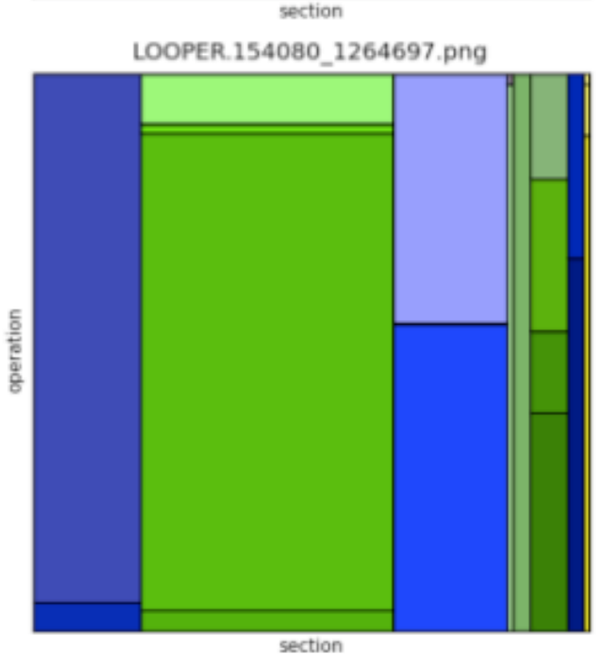

ADULTBROWSER.227364_1265996.png
operation
section

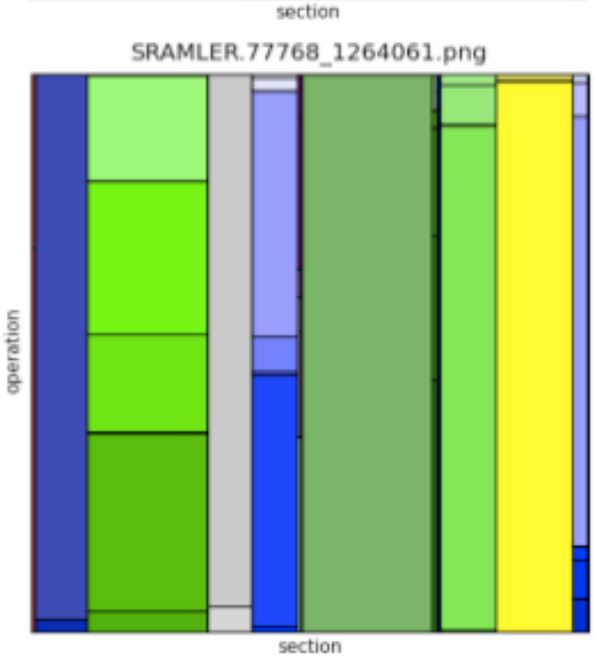

LOOPER.146883_1264370.png
operation
section

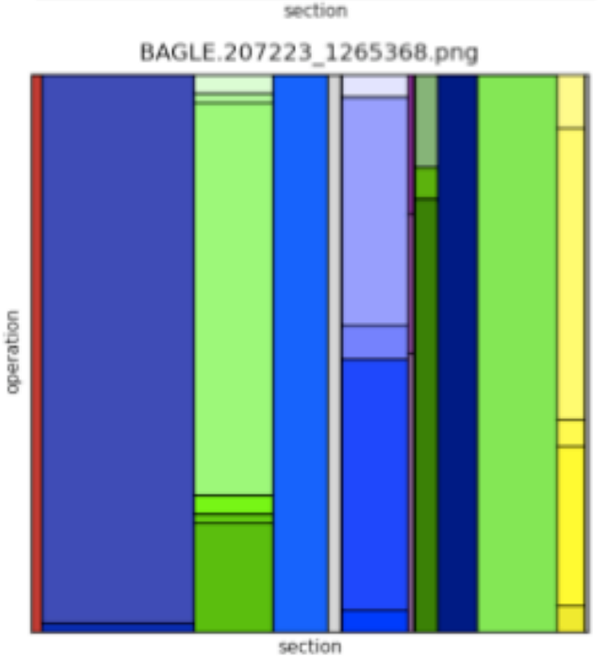

SRAMLER.77234_1264075.png
operation
section


BAGLE.207556_1265374.png
operation
section


ADULTBROWSER.227370_1266029.png
operation
section


LOOPER.154080_1264697.png
operation
section


SRAMLER.77768_1264061.png
operation
section


BAGLE.207223_1265368.png
operation
section

Assignments

Cluster 1 (968 members, 3 prototypes, 23.6% of data, 1 label, 23.6% cumulative)
mist

Cluster 2 (298 members, 8 prototypes, 7.3% of data, 1 label, 30.8% cumulative)
mist

Cluster 3 (184 members, 2 prototypes, 4.5% of data, 1 label, 35.3% cumulative)
mist

Cluster 4 (178 members, 2 prototypes, 4.3% of data, 1 label, 39.6% cumulative)
mist

Cluster 5 (145 members, 1 prototypes, 3.5% of data, 1 label, 43.1% cumulative)
mist

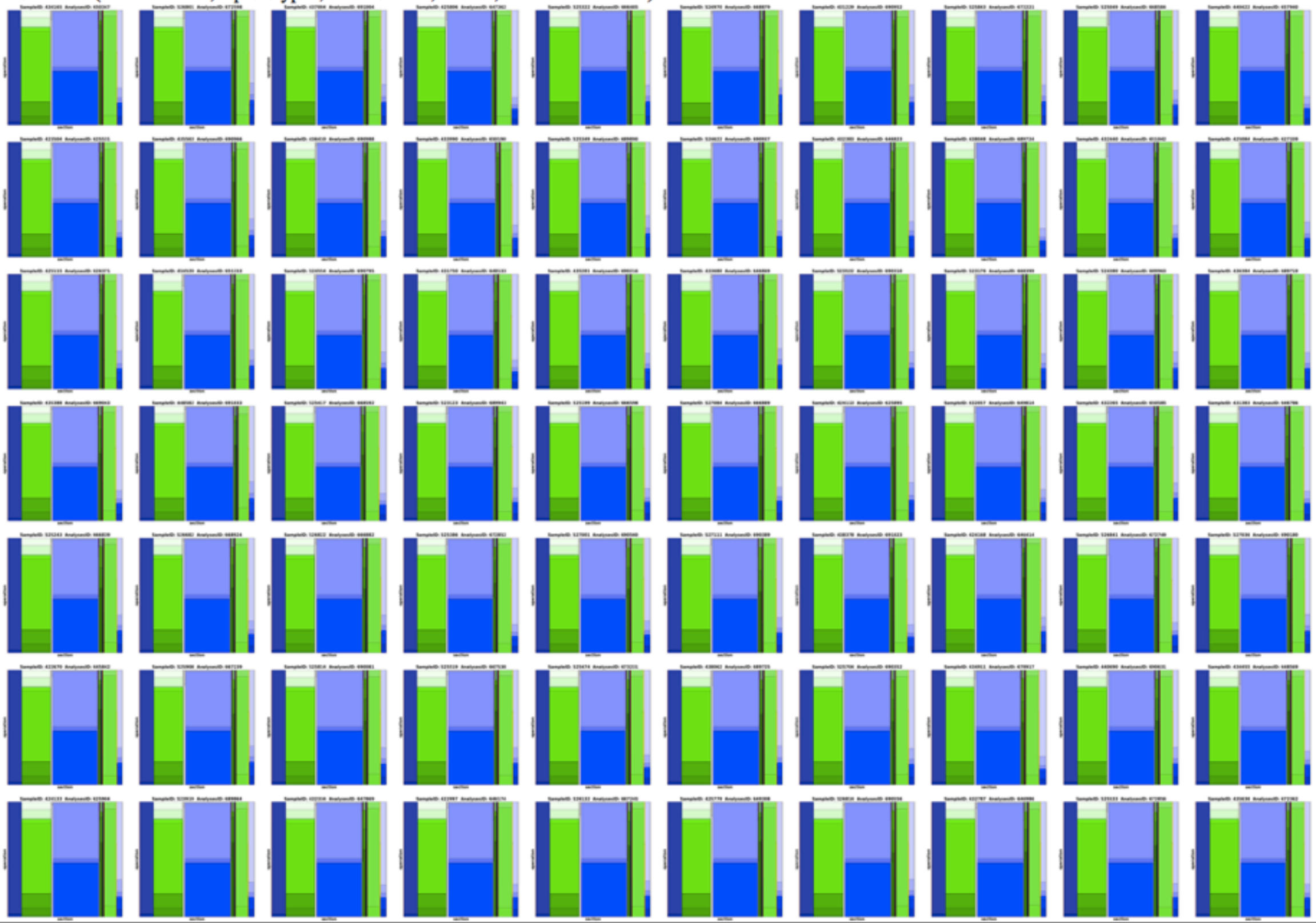
Cluster 6 (134 members, 3 prototypes, 3.3% of data, 1 label, 46.4% cumulative)
mist

Cluster 7 (133 members, 1 prototypes, 3.2% of data, 1 label, 49.6% cumulative)
mist

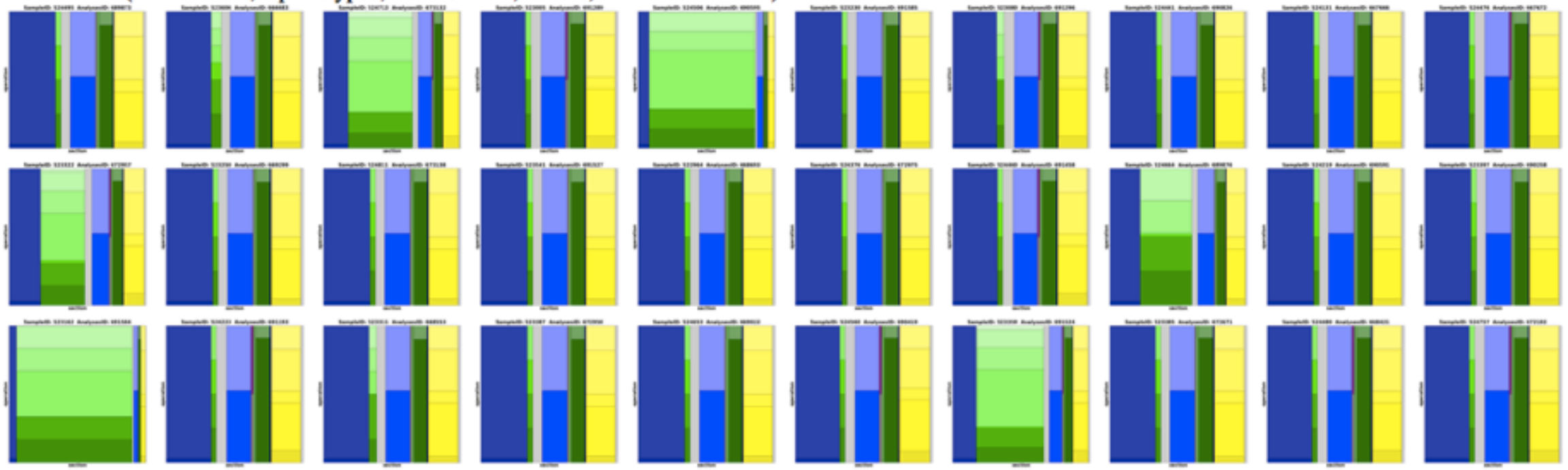
Cluster 8 (123 members, 4 prototypes, 3.0% of data, 1 label, 52.6% cumulative)
mist

Cluster 9 (103 members, 3 prototypes, 2.5% of data, 1 label, 55.1% cumulative)

- Cluster 5 (145 members, 1 prototypes, 3.5% of data, 1 label, 43.1% cumulative)



- Cluster 17 (30 members, 5 prototypes, 0.7% of data, 1 label, 64.6% cumulative)

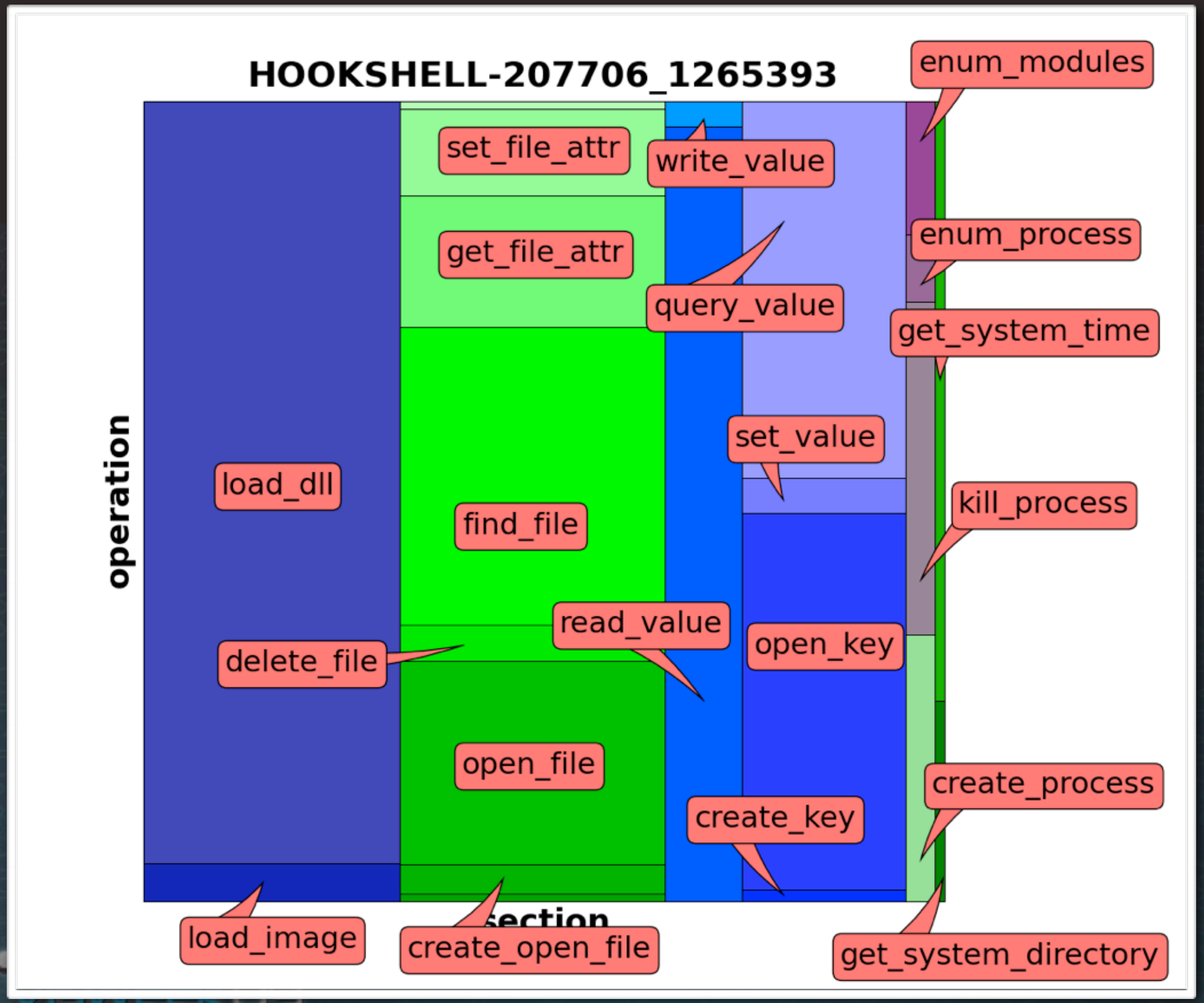


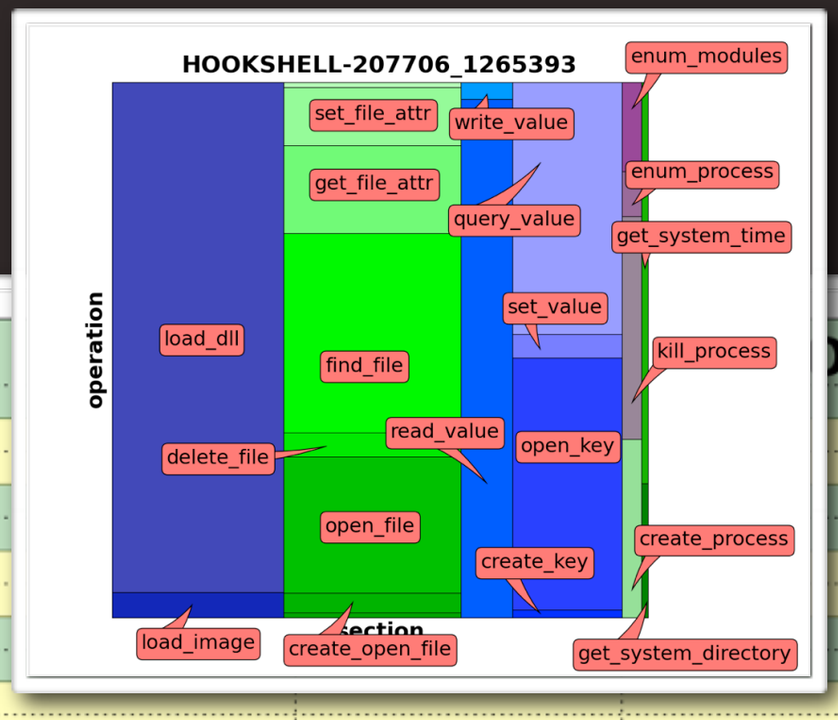
Threadgraph

- Detailed view of the monitored behavior
- Every monitored operation of all executed threads
- Sequential order preserved

- Truncated Reports only (static version)
- Zoom necessary (JavaScript)


VisWeek 09
VIS • INFOVIS • VAST


HOOKSHELL-207706_1265393
operation
section
load_dll
set_file_attr
get_file_attr
find_file
delete_file
open_file
load_image
create_open_file
write_value
query_value
read_value
set_value
open_key
create_key
enum_modules
enum_process
get_system_time
kill_process
create_process
get_system_directory



OKSHELL-207706_1265393 (level 1)

api-call sections

windows_hook
pstorage
winsock_op
window
virtual_memory
user
thread
system_info
system
service
process
registry
network
mutex
inet_helper
ini_file
icmp
filesystem
dll_handling
com

operation on registry

operation on registry

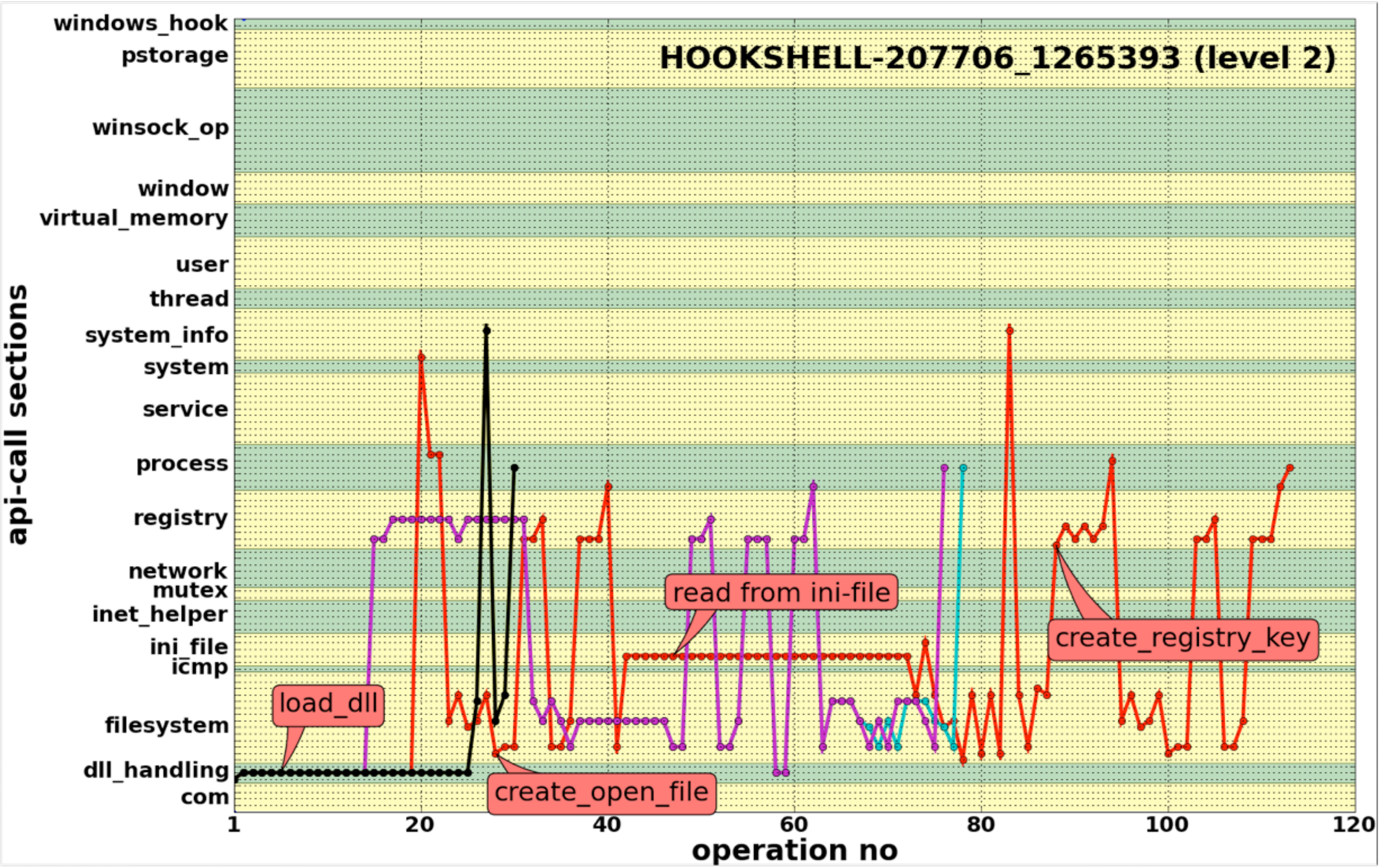
read from ini-file

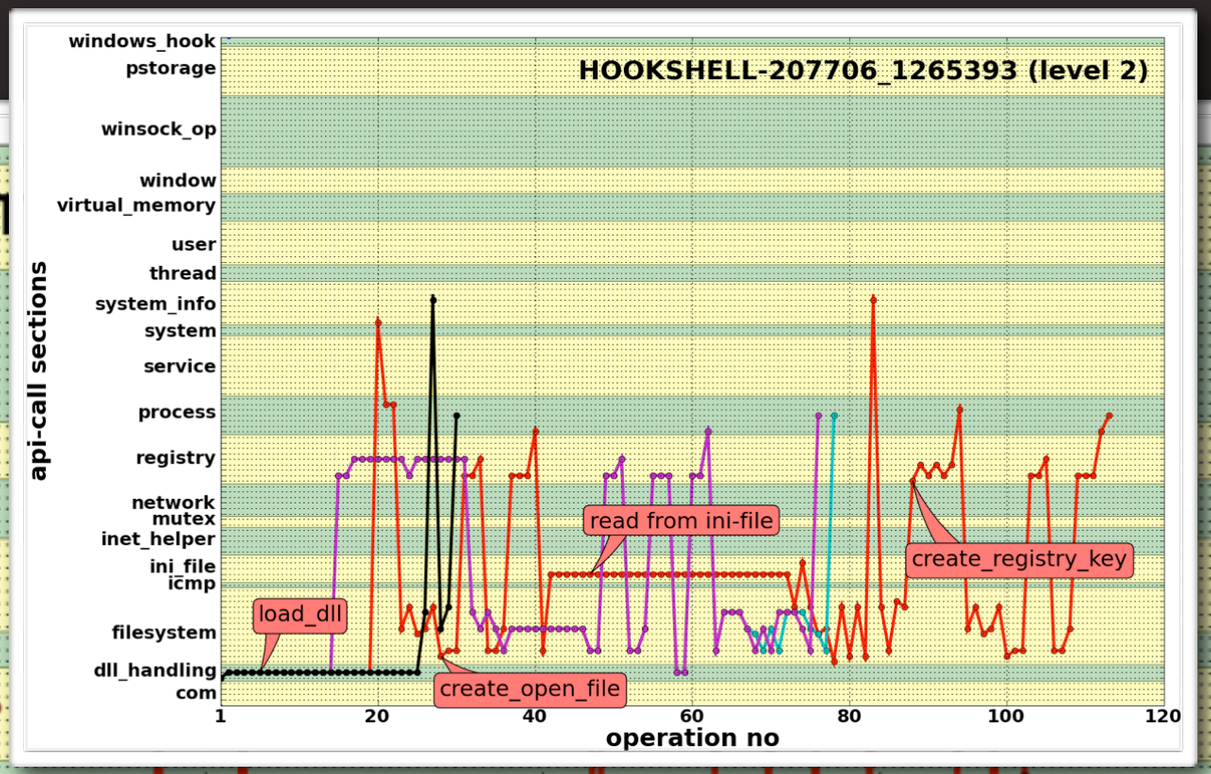
operation on filesystem

load_dll

1 20 40 60 80 100 120

operation no


HOOKSHELL-207706_1265393 (level 2)
api-call sections
windows_hook
pstorage
winsock_op
window
virtual_memory
user
thread
system_info
system
service
process
registry
network
mutex
inet_helper
ini_file
icmp
filesystem
dll_handling
com
load_dll
read from ini-file
create_registry_key
create_open_file
1
20
40
60
80
100
120
operation no


HOOKSHELL-207706_1265393 (level 2)
windows_hook
pstorage
winsock_op
window
virtual_memory
user
thread
system_info
system
service
process
registry
network
mutex
inet_helper
ini_file
icmp
filesystem
dll_handling
com
api-call sections
load_dll
create_open_file
read from ini-file
create_registry_key
1
20
40
60
80
100
120
operation no

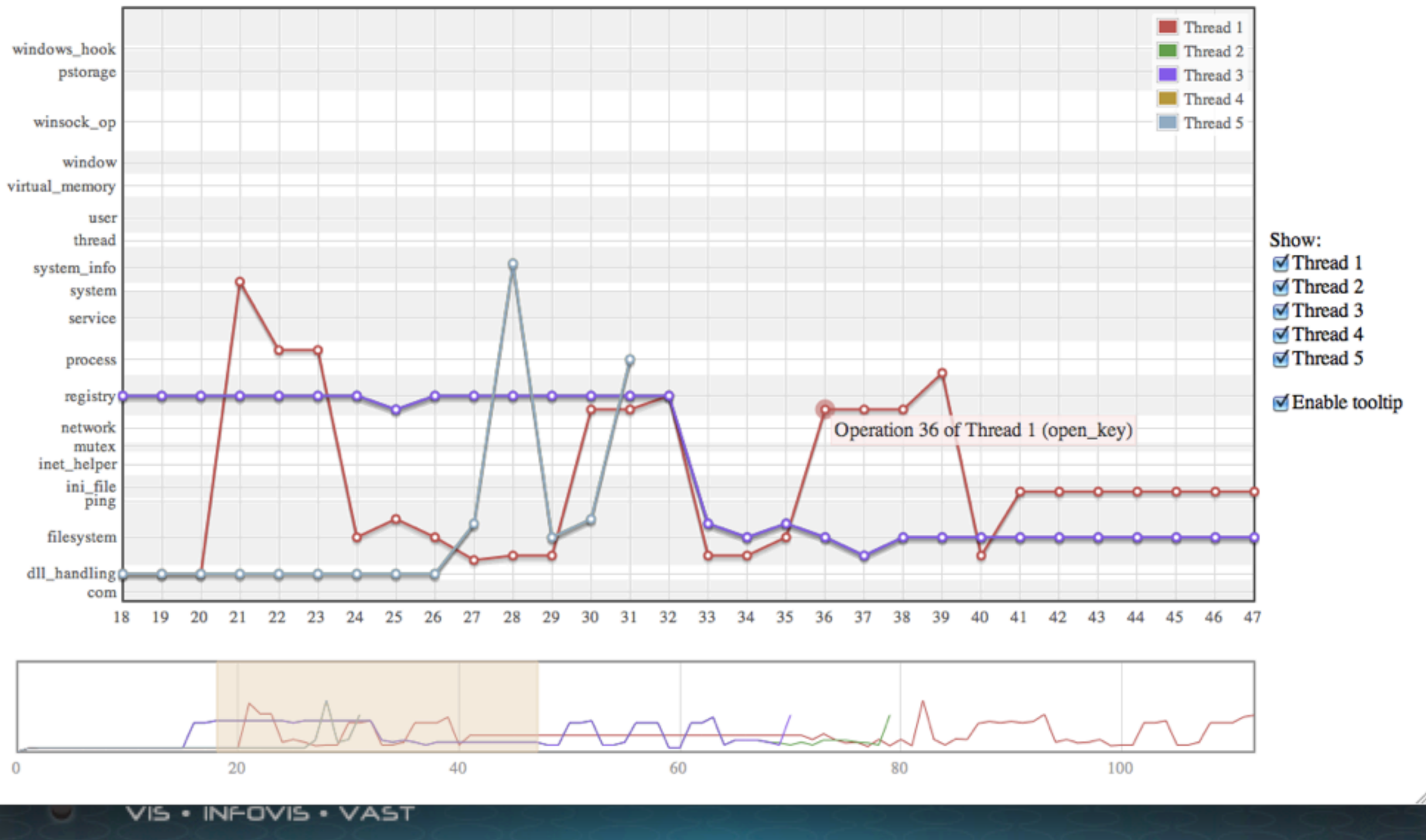
windows_hook
pstorage
winsock_op
window
virtual_memory
user
thread
system_info
system
service
process
registry
network
mutex
inet_helper
ini_file
icmp
filesystem
dll_handling
com
api-call sections
1
100
200
300
400
500
600
operation no

Threadgraph

Threadgraph

Threadgraph of SampleID: 129956 AnalysesID: 665508 (level2)

< open_key key = HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers />



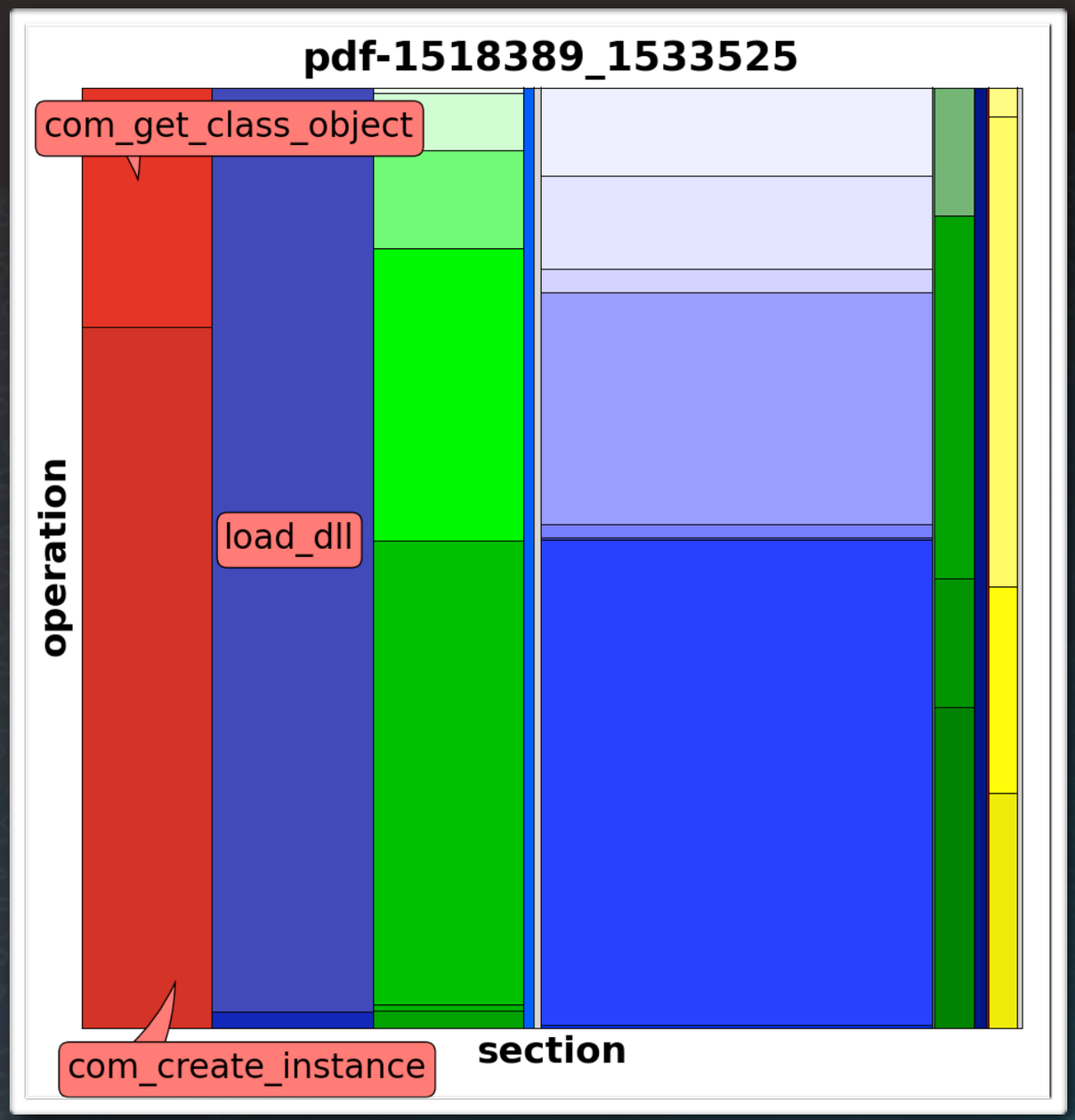
Analysis of malicious PDFs

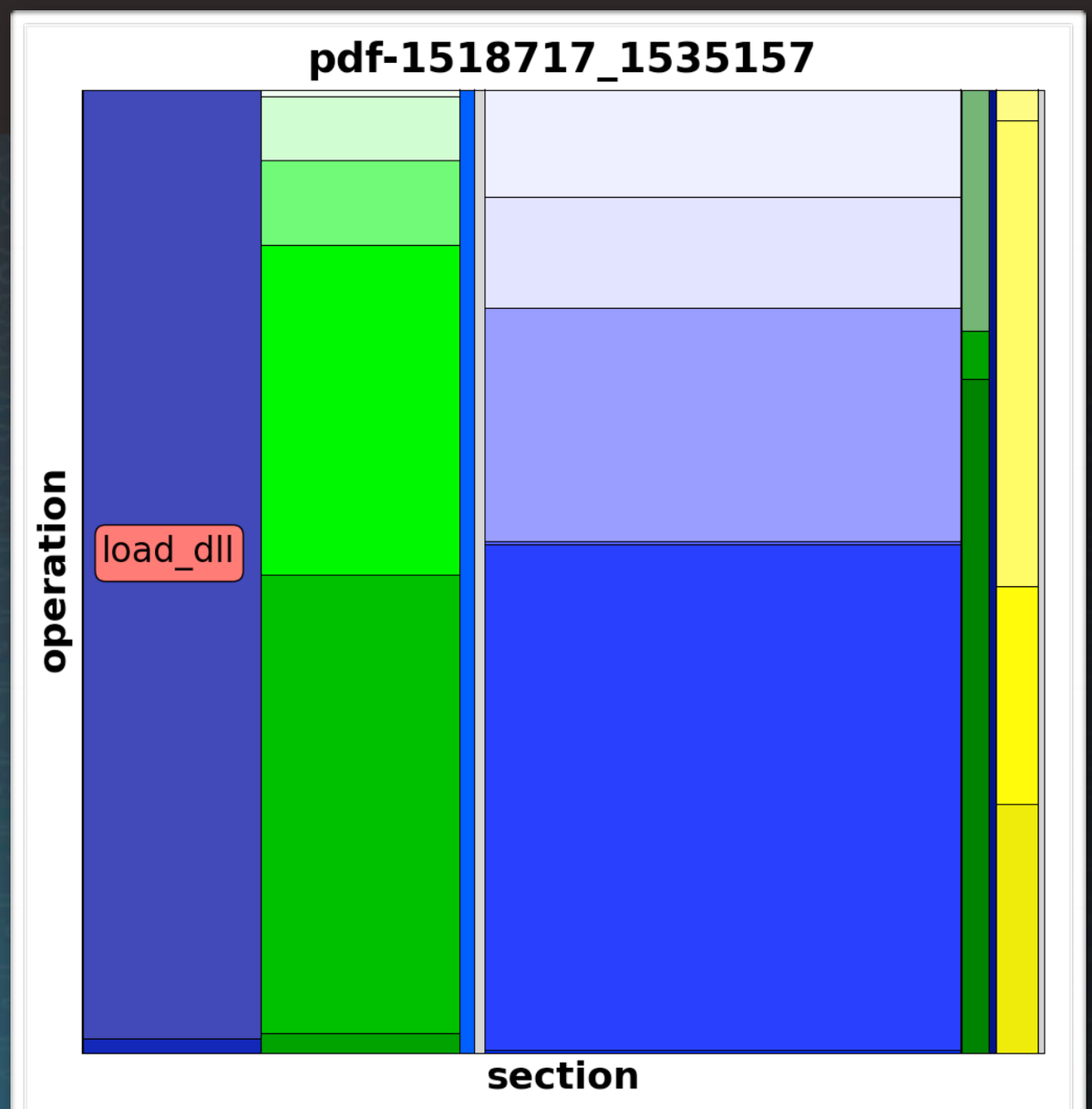
- Monitor Adobe Acrobat Reader within CWSandbox
- Autoupdate disabled

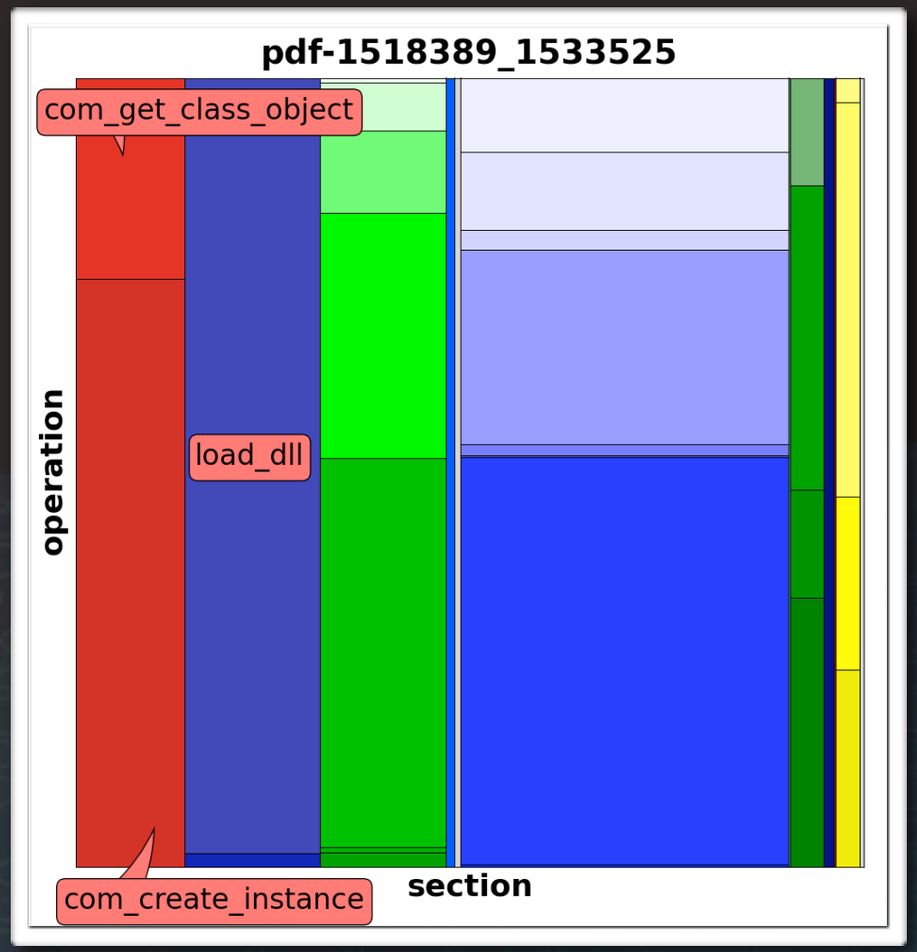
- Short experiment:
  - 200 benign PDFs
  - 17 malicious PDFs

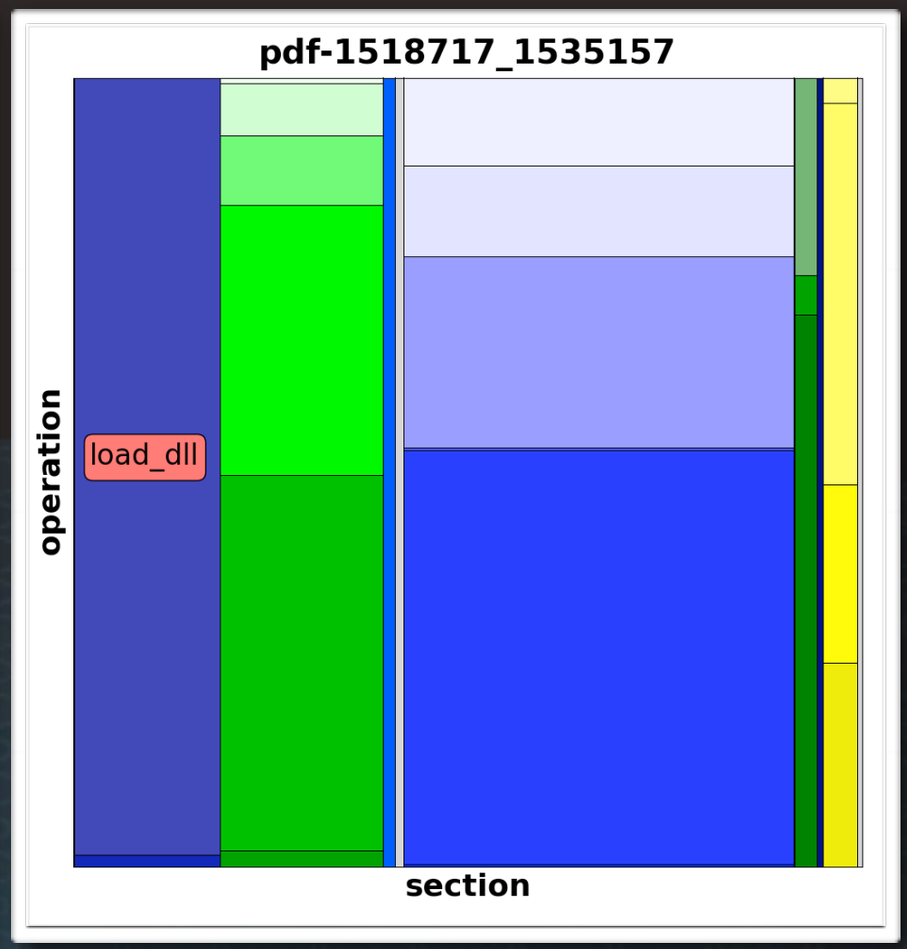
- Two different Treemaps
- Malicious operations are observable at once

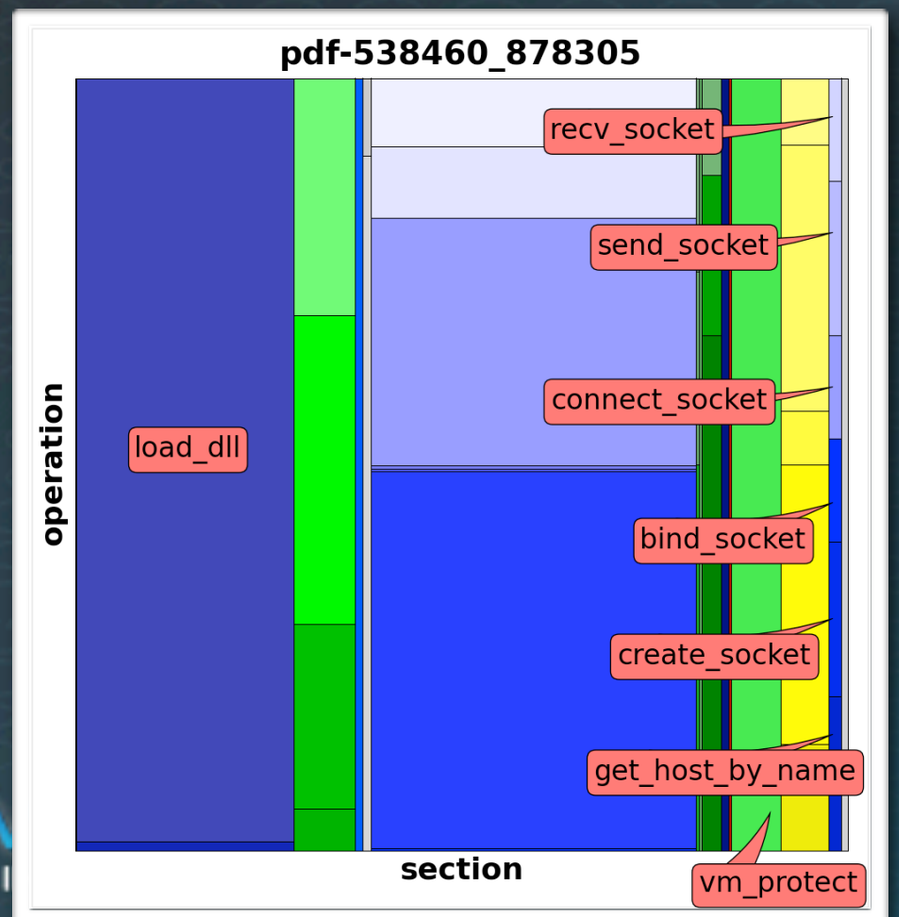

VisWeek 09
VIS • INFOVIS • VAST

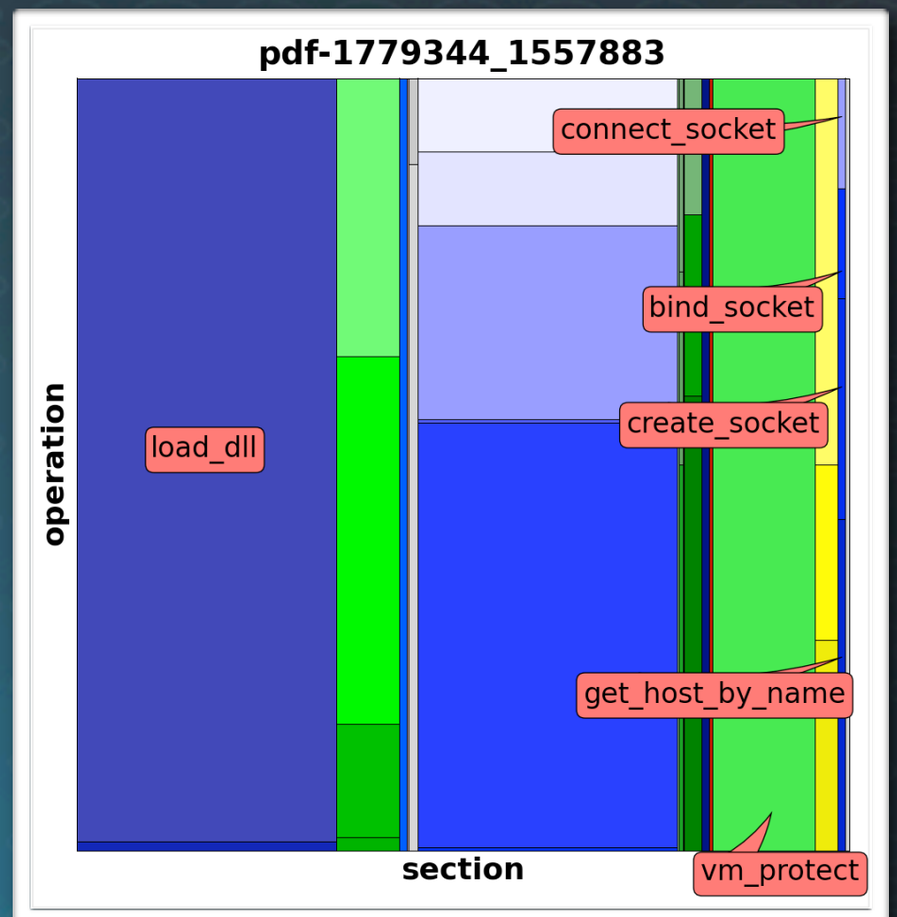


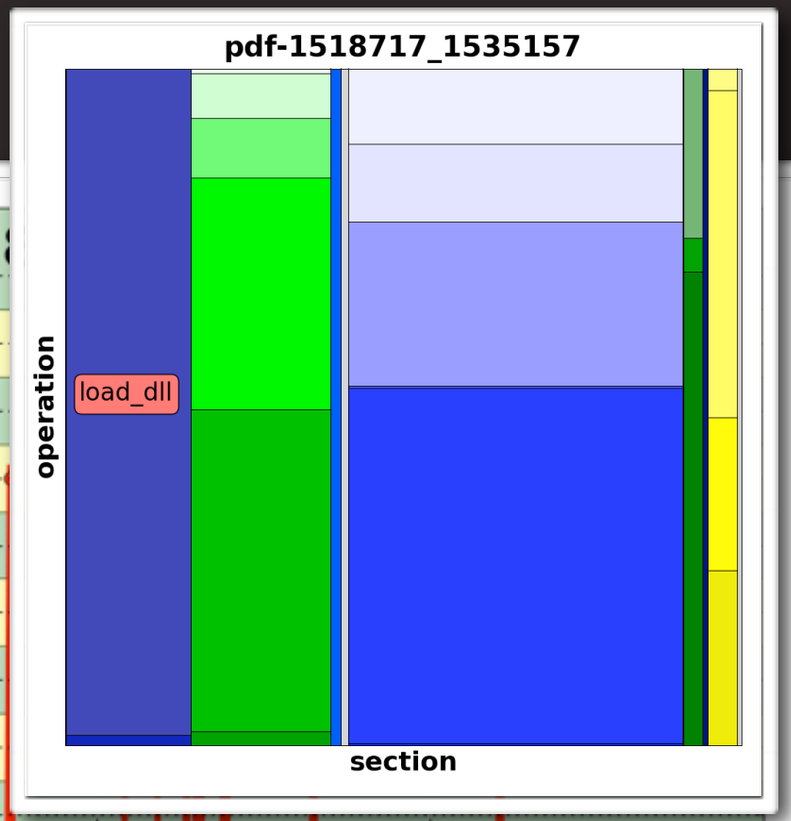



pdf-1518389_1533525
com_get_class_object
load_dll
com_create_instance
operation
section

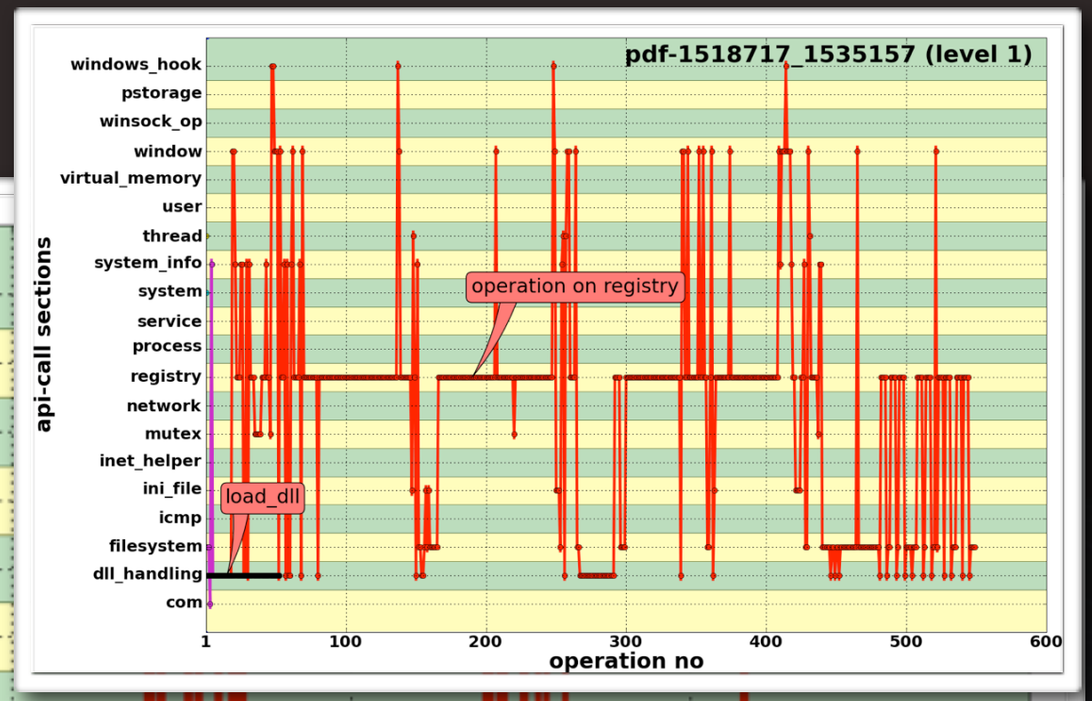

pdf-1518717_1535157
load_dll
operation
section


pdf-538460_878305
recv_socket
send_socket
connect_socket
load_dll
bind_socket
create_socket
get_host_by_name
vm_protect
operation
section


pdf-1779344_1557883
connect_socket
bind_socket
create_socket
load_dll
get_host_by_name
vm_protect
operation
section


pdf-1518717_1535157
operation
load_dll
section

pdf-151
api-call sections
windows_hook
pstorage
winsock_op
window
virtual_memory
user
thread
system_info
system
service
process
registry
network
mutex
inet_helper
ini_file
icmp
filesystem
dll_handling
com
operation on registry
load_dll
1
100
200
300
400
500
600
operation no


pdf-1518717_1535157 (level 1)
windows_hook
pstorage
winsock_op
window
virtual_memory
user
thread
system_info
system
service
process
registry
network
mutex
inet_helper
ini_file
icmp
filesystem
dll_handling
com
api-call sections
operation on registry
load_dll
1
100
200
300
400
500
600
operation no

windows_hook
pstorage
winsock_op
window
virtual_memory
user
thread
system_info
system
service
process
registry
network
mutex
inet_helper
ini_file
icmp
filesystem
dll_handling
com
api-call sections
network activity
allocate virtual memory
operation on registry
load_dll
additional load_dll
1
100
200
300
400
500
600
operation no

Conclusion

- First attempt on visualization - need Feedback
- Plots are accessible on *CWSandbox.org*
  - Static + JavaScript version

- Study on image clustering and classification
- Development of further visualization types

http://pi1.informatik.uni-mannheim.de
http://cwsandbox.org

Questions?

trinius@uni-mannheim.de

VisWeek 09
VIS • INFOVIS • VAST