

Visualization of Malware Behavior

DIMVA 2009
- Rump Session -



PiI - Laboratory for Dependable Distributed Systems

UNIVERSITÄT
MANNHEIM



Motivation

- CWSandbox.org
- Detailed behavior report
- 2.500 - 4.000 binaries a day
- Each contains several hundred of api-calls

1265393.xml

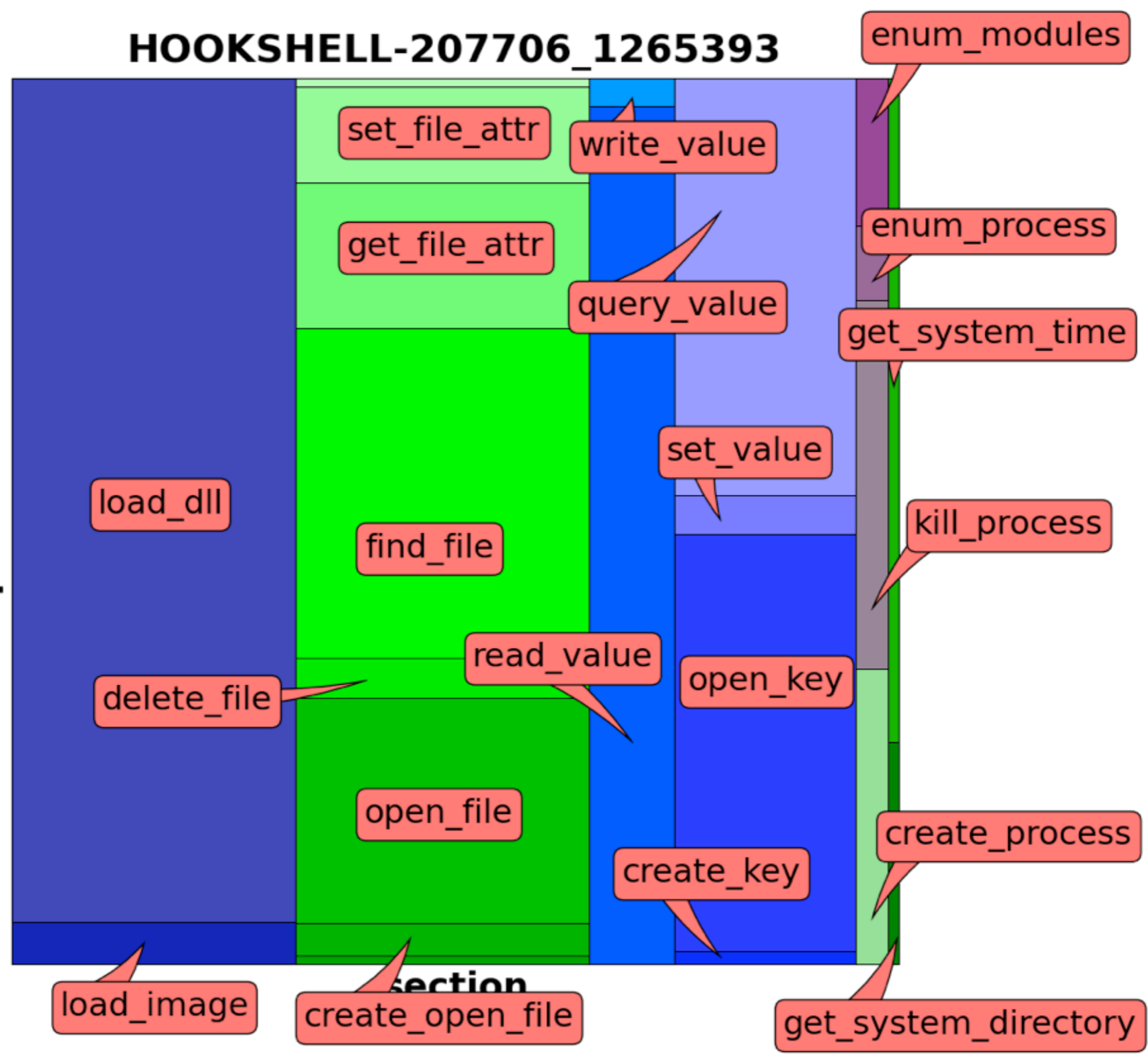
```
<?xml version="1.0"?>
<!-- This analysis was created by CWSandbox (c) CWSE GmbH / Sunbelt Software-->
<analysis cwsversion="2.1.6" time="3/28/2009 10:06:45 PM" file="C:\1265393" md5="a9f6aa1649e6a0f1bfad8a576f0193a0"
  sha1="1d13db7f7b57fcc6c715084a20660a464a7aab50" logpath="C:\cwsandbox\log\1265393\run_1\">
  <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>
    </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="cc33461f7147042c14d739ba7dc1916e6cccc8139"/>
          <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="f683eb85535e34c41e5bf5da535d9dcc4ae5e8b2"/>
          <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"/>
        </all_section>
      </thread>
    </process>
  </processes>
</analysis>
```


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"/>
<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\sysstest.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"
```


HOOKSHELL-207706_1265393

operation



section

load_image

create_open_file

get_system_directory

delete_file

load_dll

find_file

set_file_attr

get_file_attr

open_file

read_value

write_value

query_value

create_key

set_value

open_key

get_system_time

enum_process

enum_modules

kill_process

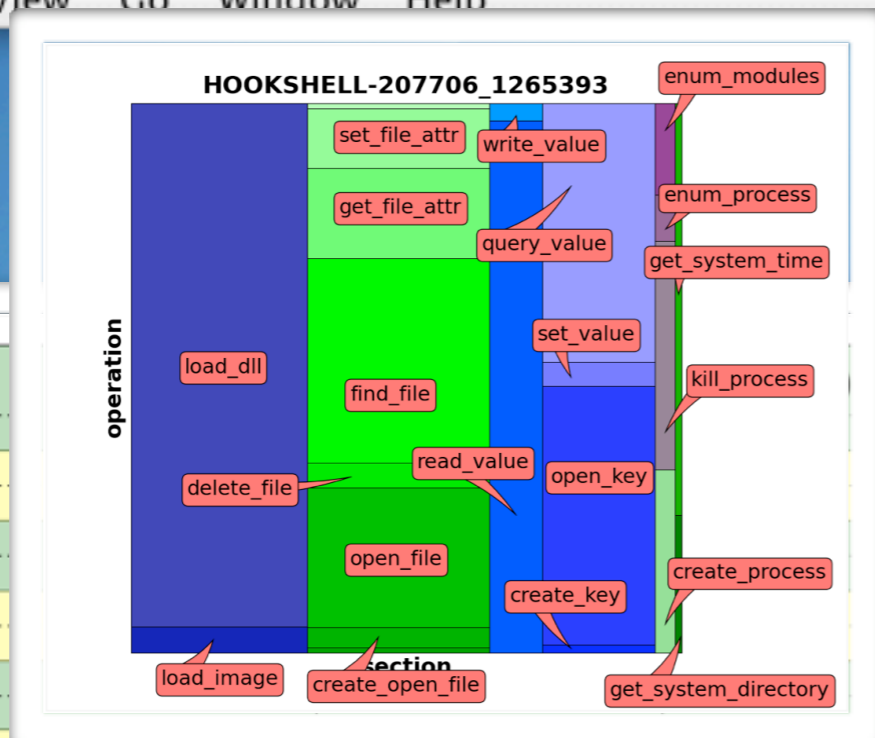
create_process

intosh HD





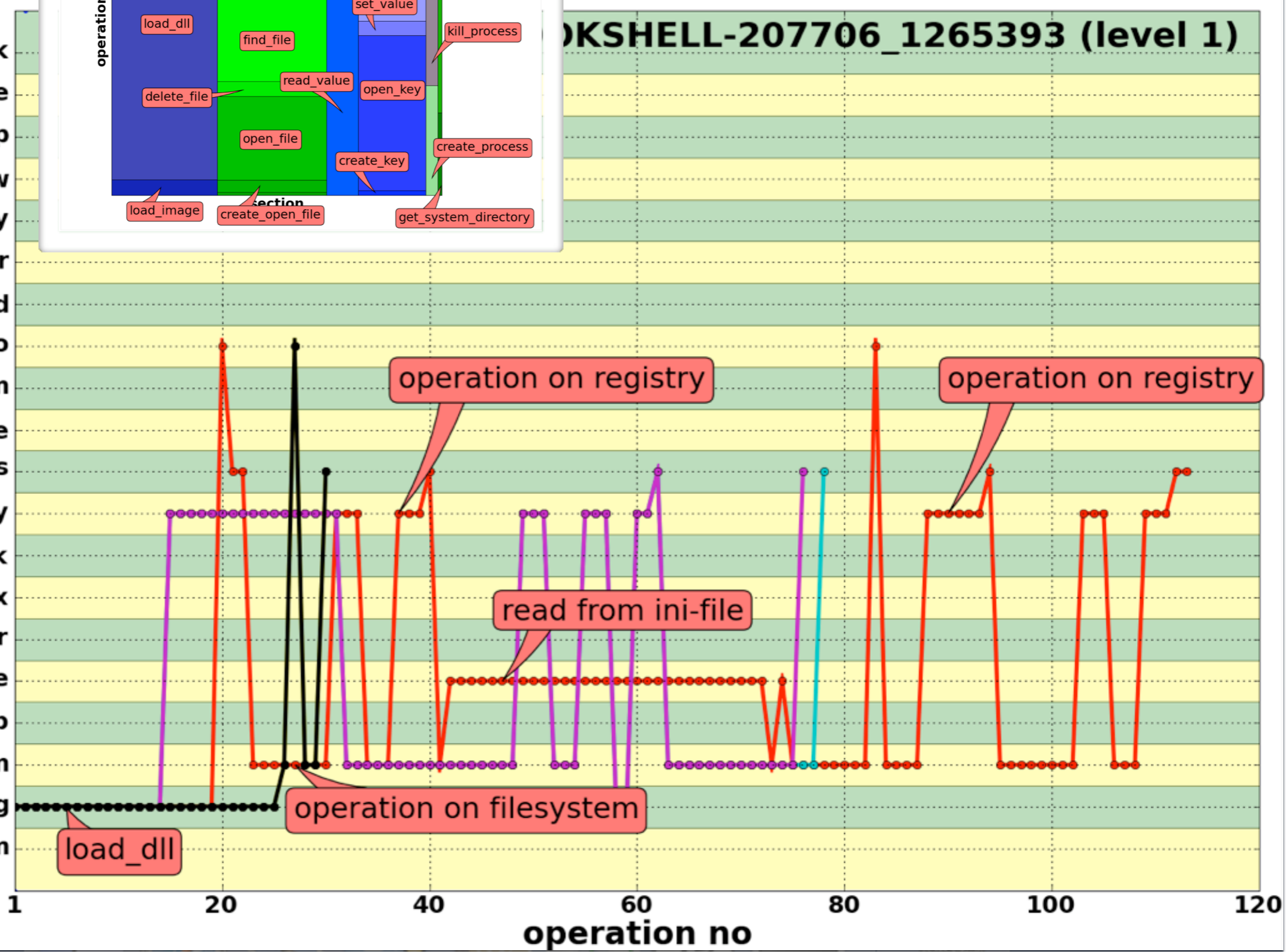
Macintosh HD



HOOKSHELL-207706_1265393 (level 1)

api-call sections

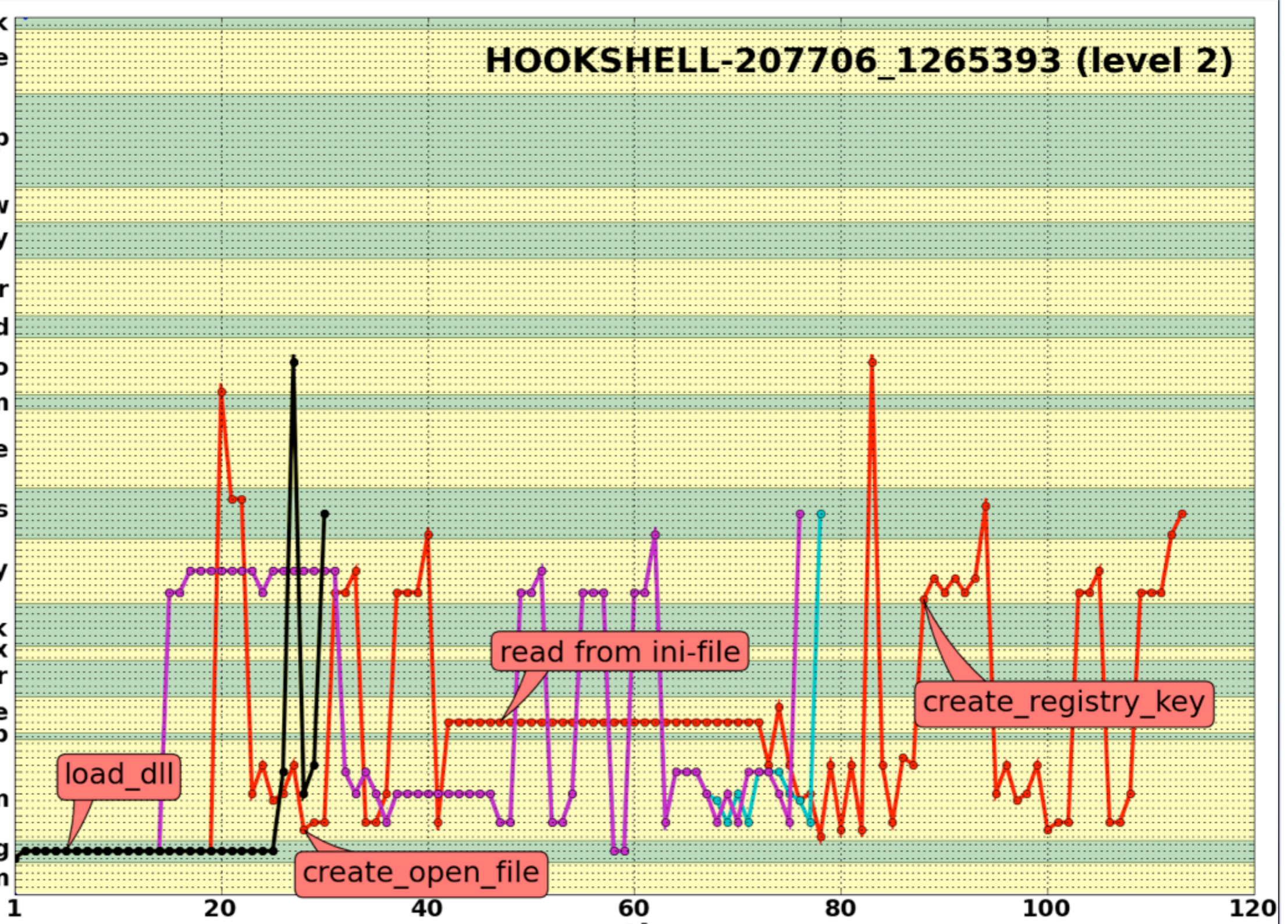
- windows_hook
- pstorage
- winsock_op
- window
- virtual_memory
- user
- thread
- system_info
- system
- service
- process
- registry
- network
- mutex
- inet_helper
- ini_file
- icmp
- filesystem
- dll_handling
- com

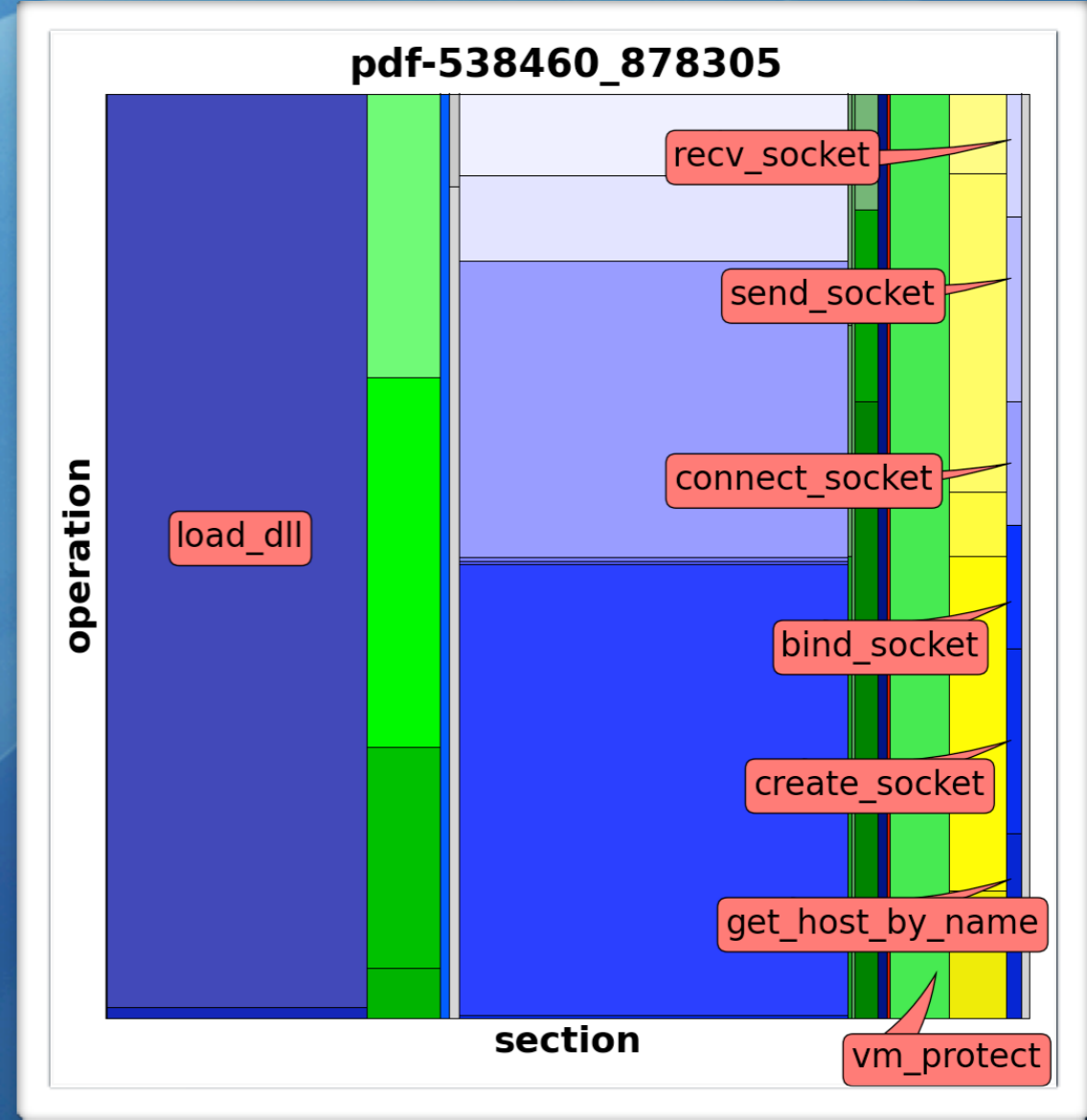
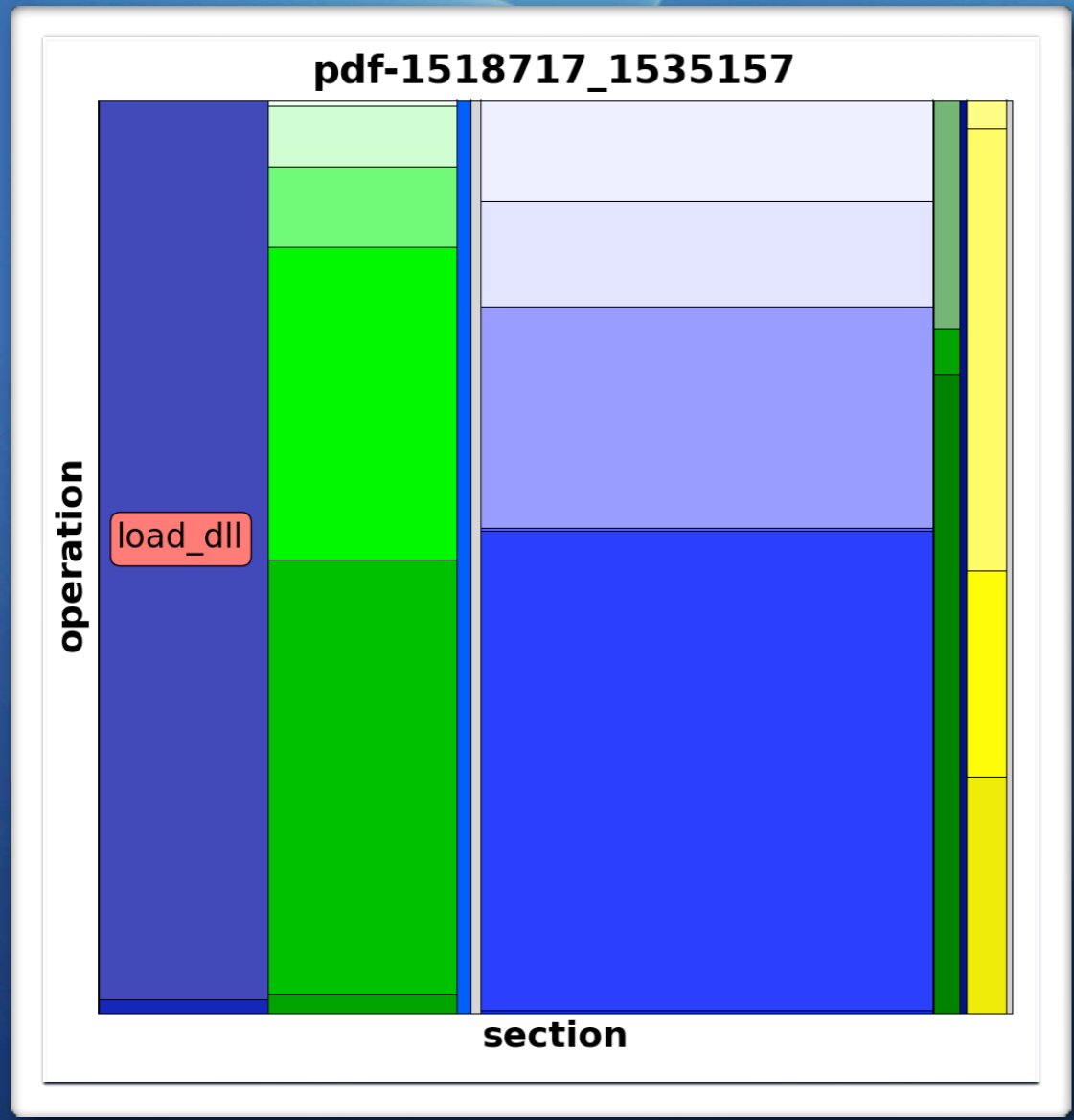


HOOKSHELL-207706_1265393 (level 2)

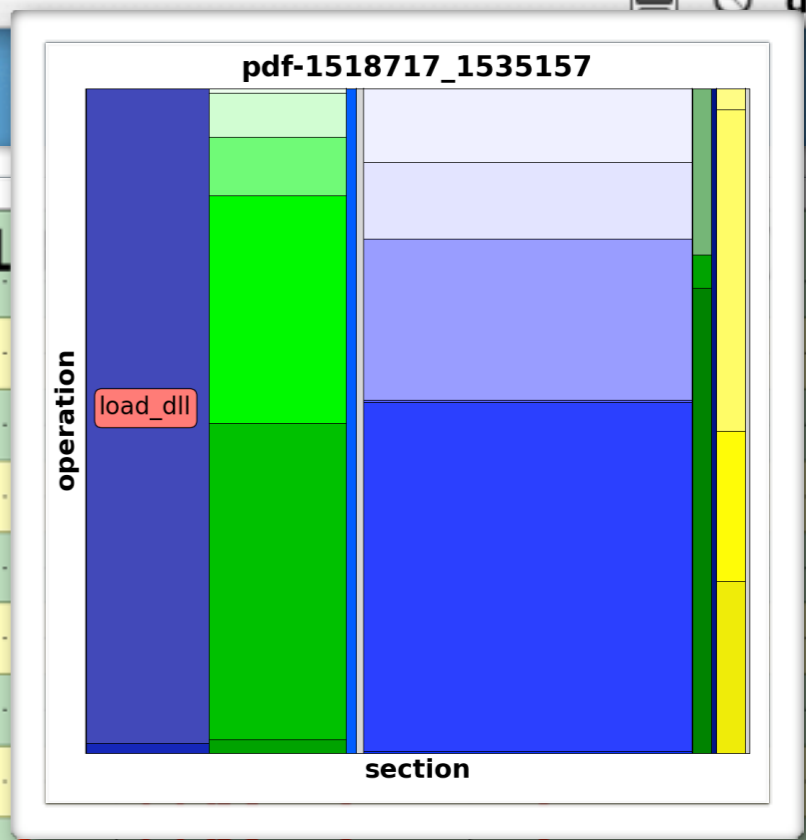
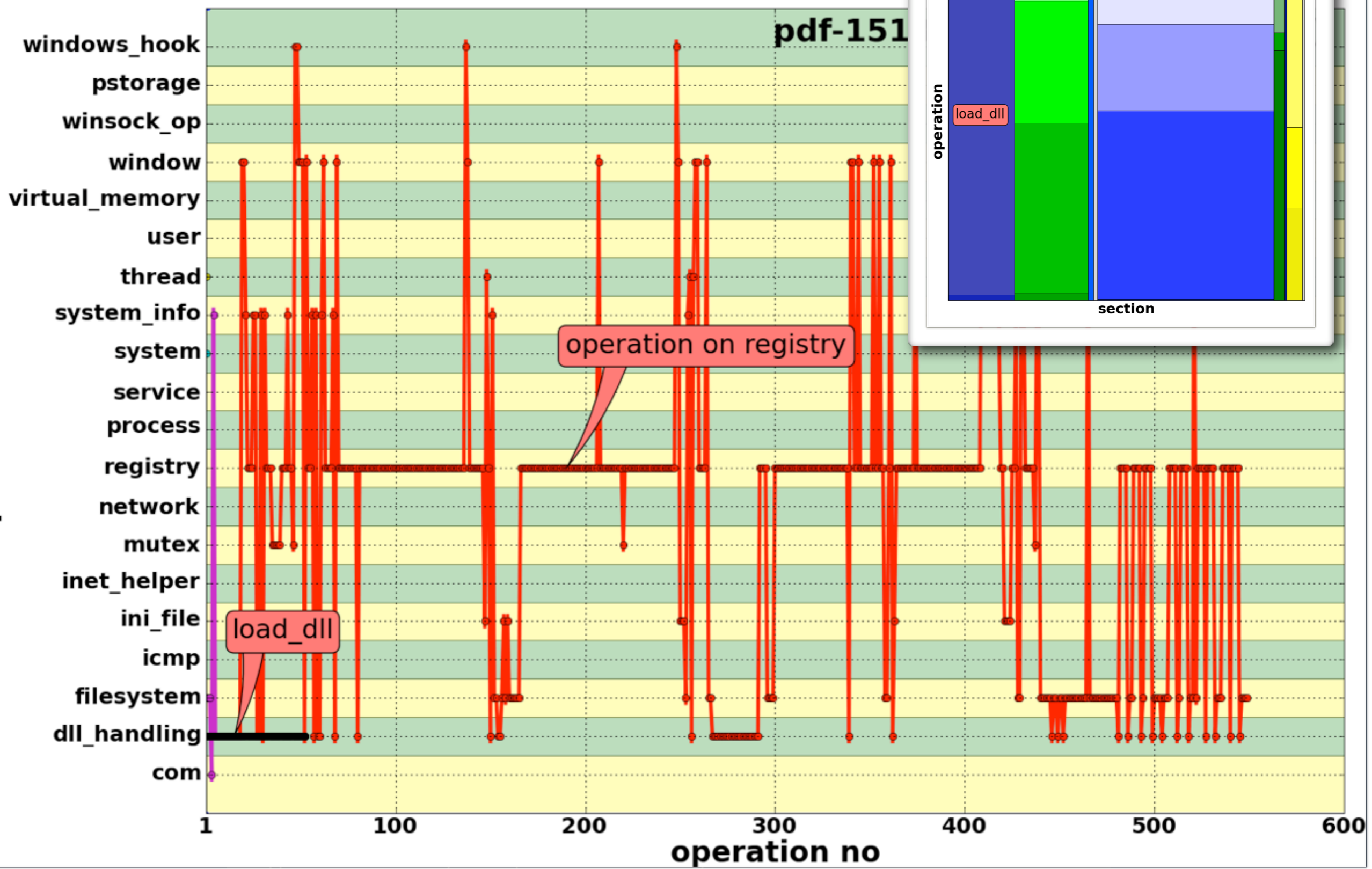
api-call sections

- 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

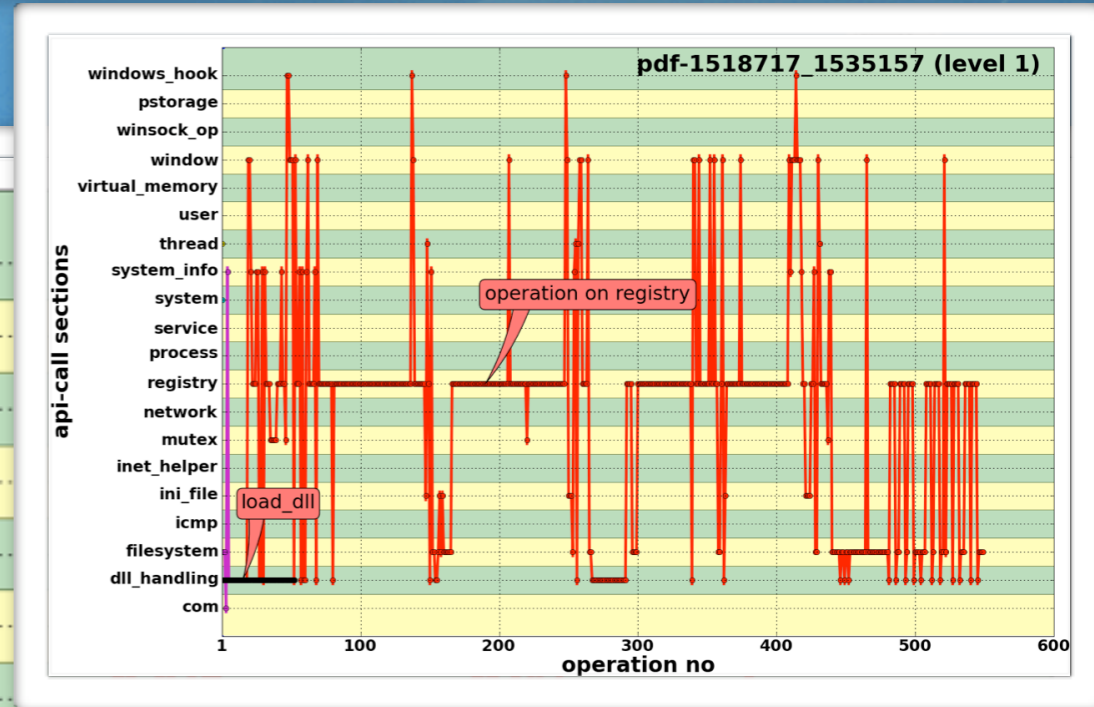
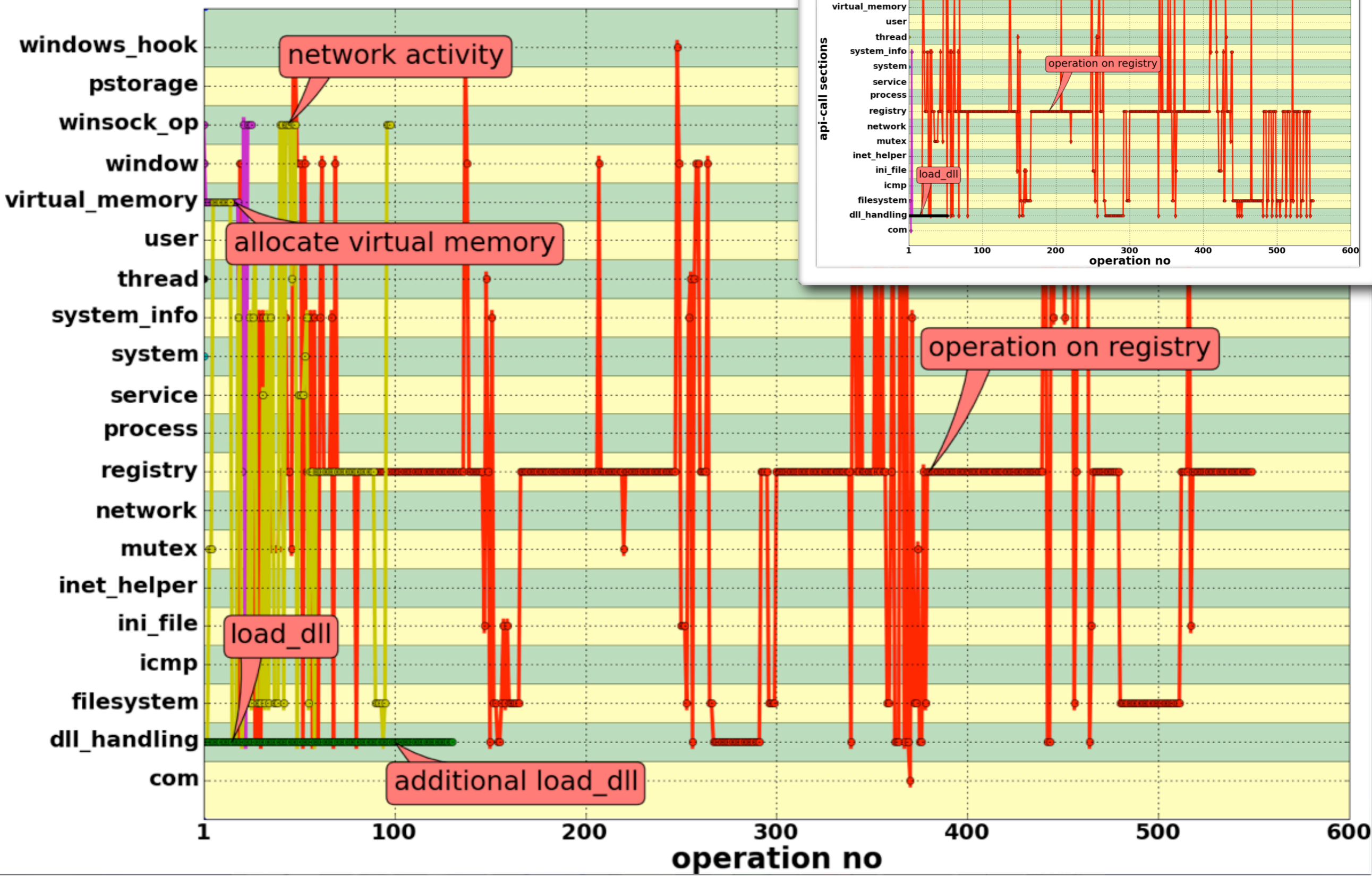




api-call sections



api-call sections





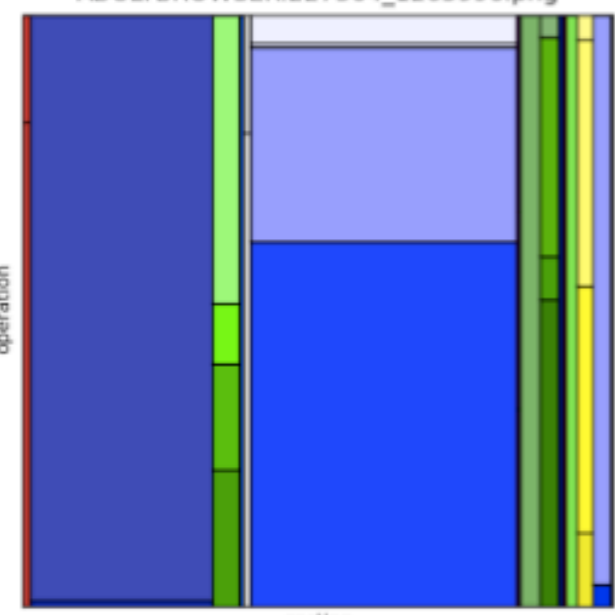
Future Work

- More / More suitable visualization techniques
- Getting feedback of other analysts
 - Include the Pics into CWSandbox.org
 - What do you think?
- Image clustering and classification



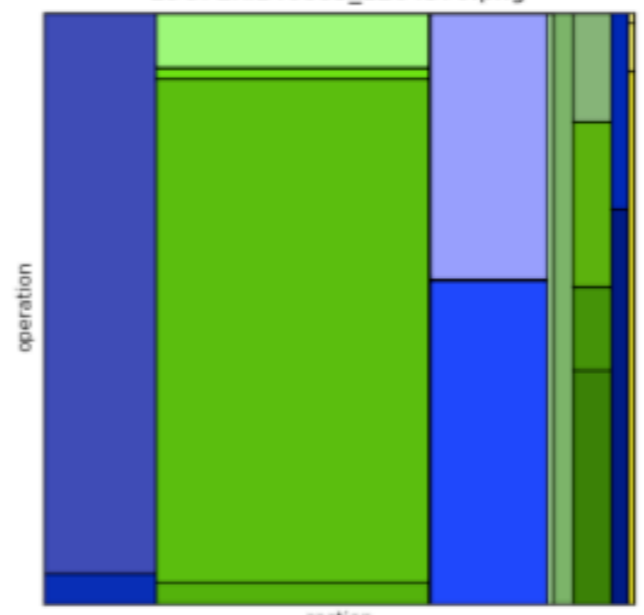
Macintosh HD

ADULTBROWSER.227364_1265996.png



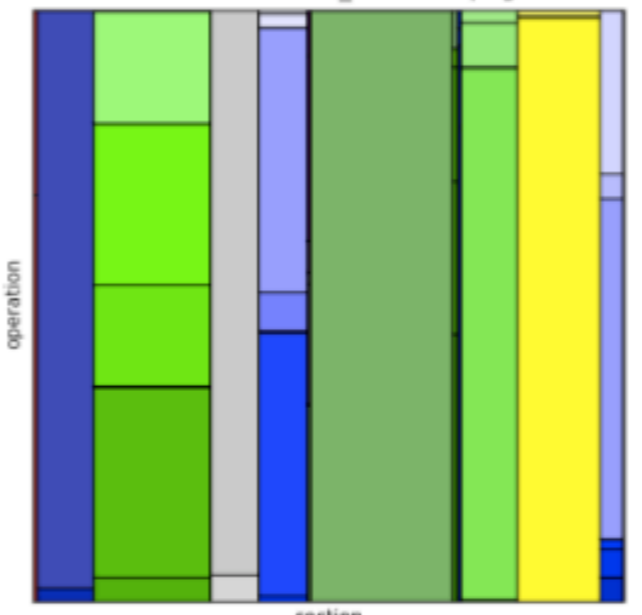
section

LOOPER.146883_1264370.png



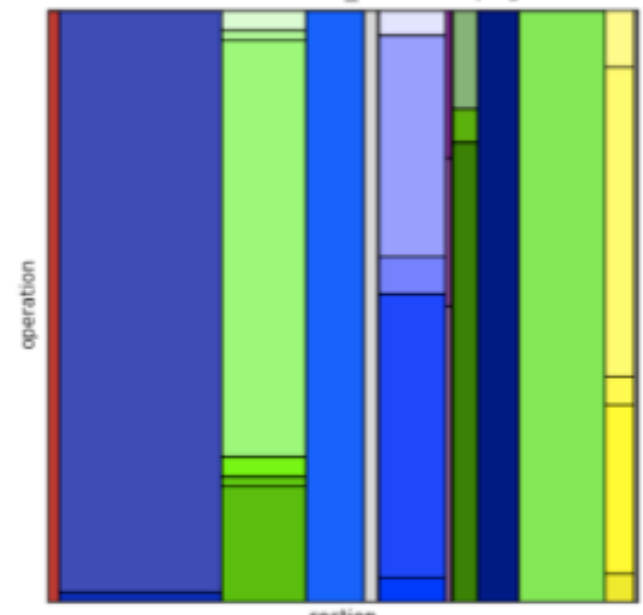
section

SRAMLER.77234_1264075.png



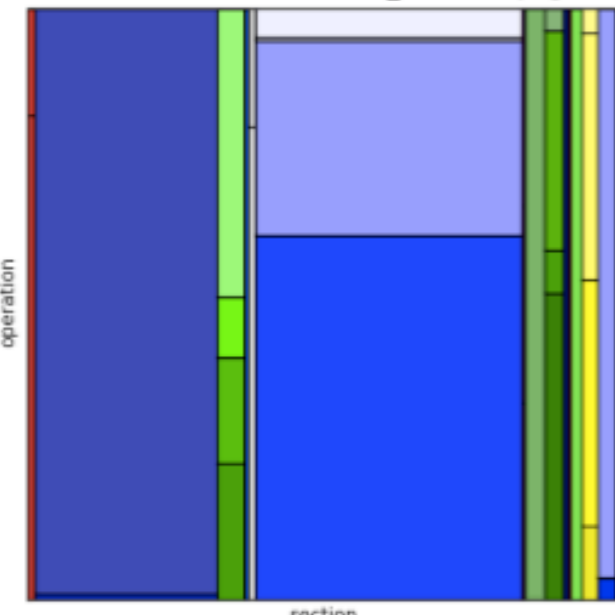
section

BAGLE.207556_1265374.png



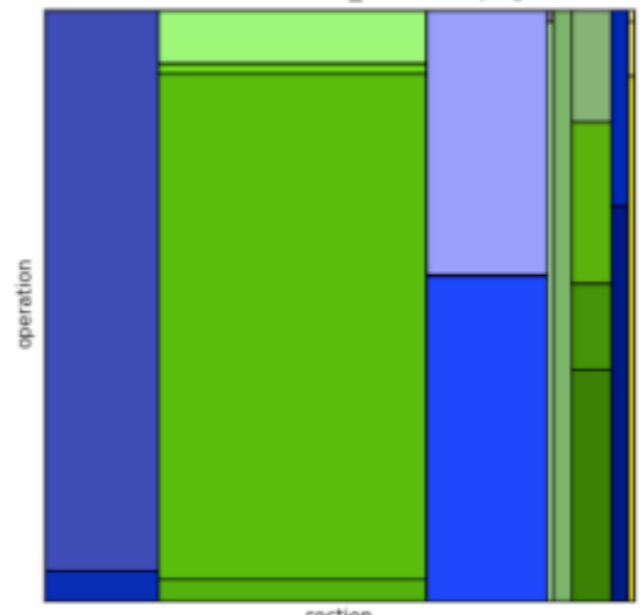
section

ADULTBROWSER.227370_1266029.png



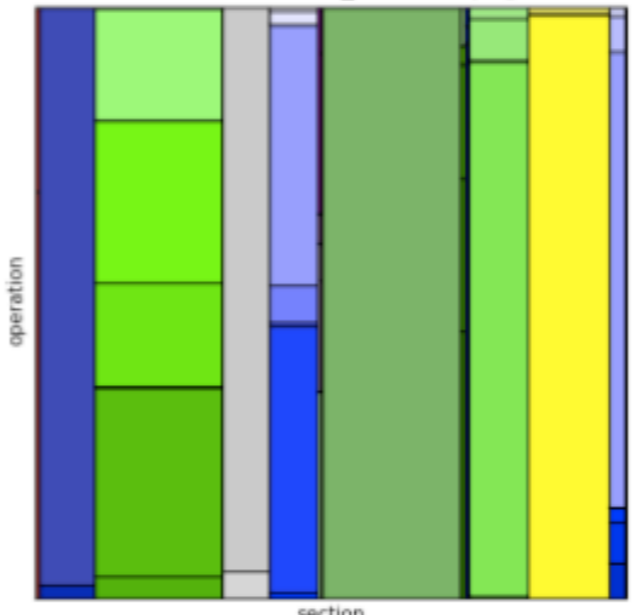
section

LOOPER.154080_1264697.png



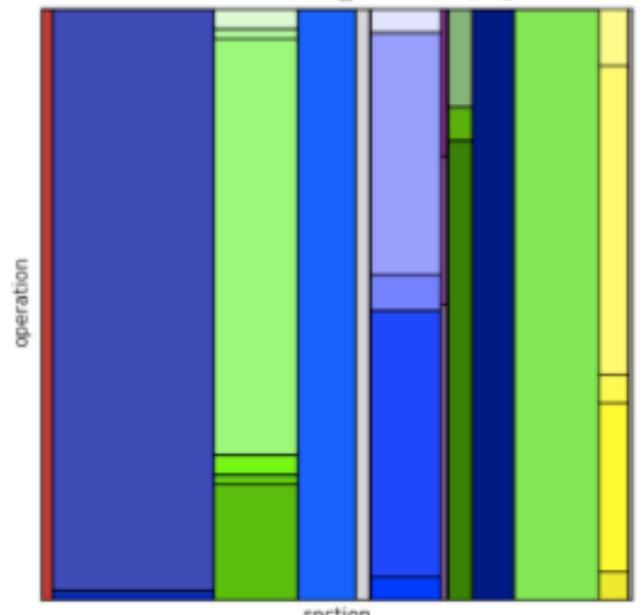
section

SRAMLER.77768_1264061.png



section

BAGLE.207223_1265368.png



section



Philipp Trinius

<http://pil.informatik.uni-mannheim.de/>
trinius@uni-mannheim.de

What do you think?



PiI - Laboratory for Dependable Distributed Systems

UNIVERSITÄT
MANNHEIM