Back to the ‘root’ of Incident Response

Boston Park Plaza Hotel | June 22-27, 2014
Merovingio: mislead the malware

Juan Carlos Montes – INTECO-CERT
Index

• Malware Analysis
  • what else?
  • state of art
  • why?
• Merovingio
  • Sandboxie
  • Merovingio Agent
• PebHooking
• DorianIA
• Merovingio Website
Index

• Malware Analysis
  • what else?
  • state of art
  • why?
• Merovingio
  • Sandboxie
  • Merovingio Agent
• PebHooking
• DorianIA
• Merovingio Website
Malware Analysis

What else?

• New techniques
• Avoid signatures
• The market is dozed
• A lot of new samples daily
• It’s expensive complicated have people focused on malware analysis in a CSIRT
Malware Analysis

State of art

• Commercial products are similar
  • Same VM.
  • Same drivers.
  • Same look&feel.
  • SAME RESULTS.

• The commercial products are the same limits
  • One sample on each VM.
    • Wait to reboot/reset the VM to start another analysis.
  • The analysis spend 2-3 minutes all times. This time is not based on the behavior of the sample.
  • Attached to the company for any grown.
  • And… the source code is not our.
Malware Analysis

Why?

• Need “anything” to detect new samples and behaviors
• Avoid the dependencies of the antivirus
• Avoid the problems with VM.
  • One sample on each VM
  • Samples are out of control on execution
• Hasten the analysis
• Include some control on the execution
• Create a system to simulate behaviors
Index

- Malware Analysis
  - what else?
  - state of art
  - why?
- Merovingio
  - Sandboxie
  - Merovingio Agent
- PebHooking
- DorianIA
- Merovingio Website
Merovingio

- “Virtual Machine”
- Sandboxie
- Pebhooking
- DorianIA

- And… his web site 😊
Merovingio

Sample → Web site → VirtualBox

Dorian IA

SandBoxie
Pebhocking
• Run programs in a sandbox
• Prevent permanent changes on system
• Help us to load our libraries on each process
• Isolate each program execution
Merovingio Agent

- Tested in Windows XP and Windows 7
- Developed in Python v2.7
- Can manage all sandboxie instances as we want
- Recover the logs and send us to next step
- Multithread
- Can receive more than one sample at the same time
- Decide on which instance must be executed the sample
  - Free slot
  - Specific analysis
- Monitorized the analysis to detected when the analysis end
Index

• Malware Analysis
  • what else?
  • state of art
  • why?

• Merovingio
  • Sandboxie
  • Merovingio Agent

• PebHooking

• DorianIA

• Merovingio Website
Pebhooking

- Published in Phrack #65
  - Dreg and [Shearer] (me)

- Modify the PEB in the process to exchange real libraries for our libraries

- All dynamic loaded libraries will be hooked

- Only is necessary repair the main IAT
Pebhooking

**PEB**
- InheritedAddressSpace
- ReadImageFileExecOptions
- BeingDebugged
- Spare
- Mutant
- ImageBaseAddress
- LoaderData

**LoaderData**
- Length
- Initialized
- SsHandle
- InLoadOrderModList
- InMemoryOrderModList
- InInitOrderModList → Flink
- ...

**LDR_MODULE**
- InLoadOrderModList
- InMemoryOrderModList
- InInitOrderModList
- ...
- BaseDllName "ntdll.dll"
- ...
- BaseDllName "xxxxxx.dll"

**LDR_MODULE**
- BaseDllName "ntdll.dll"
- BaseAddress 7C801000
- ...
- BaseDllName "kernel32.dll"
Pebhooking

• `ph_ker32.dll`
  • Export the same functions that `kernel32.dll`
    • We must do a specific dll for each service pack
  • The functions exported have the same ordinal as the original function
  • We can manage any function we want
    • Store the return value
    • Modify params in runtime
    • Block the execution on any API
Index

• Malware Analysis
  • what else?
  • state of art
  • why?

• Merovingio
  • Sandboxie
  • Merovingio Agent

• PebHooking

• DorianIA

• Merovingio Website
Dorian IA

• It is based on the workflows of neural networks
• Set the time on each log received
• Analyze the log looking for patterns
• Create execution blocks
• Try to link the different blocks to create behaviors
• Show the results in a new log that is send to the website
• At this moment can learn new behaviors, our aim is create a real AI
DorianIA

Log from PebHooking

- LoadLibraryW | IMM32.DLL
- CreateFileW | C: \ikkka.exe | 0x178
- CreateFileW | COMCTL32.DLL | 0x4C
- LoadLibraryW | user32.dll
- WriteFile | 0x178 | 0x22800 | XXXXXXXXXXX
- CloseHandle | 0x4C
- CloseHandle | 0x178

Block

- CreateFileW | C: \ikkka.exe | 0x178
- WriteFile | 0x178 | 0x22800 | XXXXXXXXXXX
- CloseHandle | 0x178
Log from PebHooking

LoadLibraryW | IMM32.DLL
CreateFileW | C:\itself.exe | 0x77
ReadFile | 0x22800 | XXXXXXXXX
CloseHandle | 0x77
DeleteFile | C:\autoexec.bat
CreateFileW | C:\ikka.exe | 0x178
CreateFileW | COMCTL32.DLL | 0x4C
LoadLibraryW | user32.dll
WriteFile | 0x178 | 0x22800 | XXXXXXXXX
CloseHandle | 0x4C
CloseHandle | 0x178

Block
CreateFileW | C:\itself.exe | 0x77
ReadFile | 0x22800 | XXXXXXXXX
CloseHandle | 0x77

Block
CreateFileW | C:\ikka.exe | 0x178
WriteFile | 0x178 | 0x22800 | XXXXXXXXX
CloseHandle | 0x178

Block
DeleteFile | C:\autoexec.bat

• Read itself
• Write itself in other file
• Similar content: we use ssdeep to compare the information with threshold 95%

The sample was copied itself to another path.
Index

• Malware Analysis
  • what else?
  • state of art
  • why?
• Merovingio
  • Sandboxie
  • Merovingio Agent
• PebHooking
• DorianIA
  • **Merovingio Website**
Website features

• User management
• Able to upload different samples at same time
• Hold the history to recover old reports
• Able to looking samples for filename or hash (SHA1)
• All the communication with the agent is transparent to user
• Easy to get if any sample if malicious or not, directly from the history
Merovingio screenshots

Home page / Send samples

New analysis

Choose files

Analyze

Logged in as admin
© INTECO - CERT 2014
Merovingio screenshots

History

<table>
<thead>
<tr>
<th>ID</th>
<th>Rate</th>
<th>Hash</th>
<th>User</th>
<th>Date</th>
<th>Remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td></td>
<td>9f37021ec019cc6c01247ddbcf8474a5a0540b0</td>
<td>admin</td>
<td>16/05/2014 14:20</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>984e71ec6b2b93fd7d2ca40029a78f328a780a58</td>
<td>api</td>
<td>16/05/2014 14:20</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>ofd7575e7482d3505613d2d4ef721a3f459b98c5</td>
<td>admin</td>
<td>23/05/2014 10:36</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>5814e91b6276f4de8b7951c968f2f190a3978d</td>
<td>admin</td>
<td>26/05/2014 18:19</td>
<td></td>
</tr>
</tbody>
</table>

Logged in as admin

© INTECO - CERT 2014
Merovingio screenshots

Raw log

2014-03-10 14:46:30.35600 0xf4 zeus.exe|Sleep|20
2014-03-10 14:46:30.36700 0xf4 zeus.exe|Sleep|20
2014-03-10 14:46:30.37700 0xf4 zeus.exe|Sleep|20
2014-03-10 14:46:30.38700 0xf4 zeus.exe|Sleep|20
2014-03-10 14:46:30.39700 0xf4 zeus.exe|Sleep|20
2014-03-10 14:46:30.40700 0xf4 zeus.exe|Sleep|20
2014-03-10 14:46:30.41700 0xf4 zeus.exe|CreateFileW C:\zeus.exe|0x174
2014-03-10 14:46:30.41700 0xf4 zeus.exe|ReadFile|0x174|0x22800|TVoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
2014-03-10 14:46:30.43700 0xf4 zeus.exe|CloseHandle|0x174
2014-03-10 14:46:30.52700 0xf4 zeus.exe|CreateFileW C:\Documents and Settings\Tecnico\Datos de programa\Tysov\ovcu.exe|0x174
2014-03-10 14:46:30.52700 0xf4 zeus.exe|WriteFile|0x174|0x22800|TVoAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
2014-03-10 14:46:30.52700 0xf4 zeus.exe|CloseHandle|0x174
2014-03-10 14:46:30.52700 0xf4 zeus.exe|CreateFileW C:\Documents and Settings\Tecnico\Datos de programa\Tysov\ovcu.exe|0x174
2014-03-10 14:46:30.53700 0xf4 zeus.exe|CreateFileW C:\Documents and Settings\Tecnico\Datos de programa\Tysov\ovcu.exe|0x174
2014-03-10 14:46:30.53700 0xf4 zeus.exe|CloseHandle|0x174
2014-03-10 14:46:30.53700 0xf4 zeus.exe|CreateFileW C:\Documents and Settings\Tecnico\Datos de programa\Tysov\ovcu.exe|0x174
2014-03-10 14:46:30.53700 0xf4 zeus.exe|CloseHandle|0x174
2014-03-10 14:46:30.53700 0xf4 zeus.exe|CreateFileW C:\Documents and Settings\Tecnico\Datos de programa\Tysov\ovcu.exe|0x174
2014-03-10 14:46:30.53700 0xf4 zeus.exe|CloseHandle|0x174
2014-03-10 14:46:30.53700 0xf4 zeus.exe|CreateFileW C:\Documents and Settings\Tecnico\Datos de programa\Tysov\ovcu.exe|0x174
2014-03-10 14:46:30.53700 0xf4 zeus.exe|CloseHandle|0x174
2014-03-10 14:46:30.53700 0xf4 zeus.exe|MapViewOfFile|0x180|0x22800
2014-03-10 14:46:30.53700 0xf4 zeus.exe|CloseHandle|0x180
2014-03-10 14:46:30.58700 0xf4 zeus.exe|CloseHandle|0x188
2014-03-10 14:46:30.58700 0xf4 zeus.exe|MapViewOfFile|0x18c|0x22800
2014-03-10 14:46:30.58700 0xf4 zeus.exe|CloseHandle|0x18c
Merovingio screenshots

Analysis

Result: MALWARE

- INIT IA
  - ANALYSING PROCESSES: 2
  - ANALYSING PROCS: 230
  - CREATING BLOCKS: 142
  - LOADING RULES: rules.xml
  - MALICIOUS BEHAVIOURS DETECTED
    - SELF-REPLICATE
      - [97%]: "C:\Merovingio\Analizando\854b6605d6d318ce01336d0212412a9f04f37021ee819cc6c01247ddbcf474a5a8540b8.exe" -> "C:\Docu
  - TRY TO READ/WRITE OTHER PROCESS
  - TRY TO FOUND WINLOGON.EXE
  - MULTIPLE OPENPROCESS CALLED

- OTHER INFORMATION
  - MODIFIED FILES IN "Documents And Settings"
    - "C:\Documents and Settings\technico\datos de programa\okzyv\uczy1.exe"
  - MULTIPLE CALLS TO SLEEP

Details

<table>
<thead>
<tr>
<th>User</th>
<th>admin</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA1</td>
<td>94f37021ee819cc6c01247ddbcf474a5a8540b8</td>
</tr>
<tr>
<td>Rate</td>
<td>MALWARE</td>
</tr>
<tr>
<td>Date</td>
<td>2014-05-27 13:45:22.868193+00:00</td>
</tr>
</tbody>
</table>

Remove [Remove]
Merovingio screenshots

API

My API Key

<table>
<thead>
<tr>
<th>Public API</th>
<th>d18271a2d52815778cf681707c844667b9d5c255</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Key enabled</td>
</tr>
</tbody>
</table>

Settings

<table>
<thead>
<tr>
<th>Url</th>
<th>Explain</th>
<th>Allow Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>api/get-token/</td>
<td>Uses this url to get your token</td>
<td>POST</td>
</tr>
<tr>
<td>api/report/</td>
<td>Uses this url to send samples</td>
<td>POST</td>
</tr>
<tr>
<td>api/report/sha1/(Your SHA1)</td>
<td>Uses this url to search using SHA1</td>
<td>GET</td>
</tr>
<tr>
<td>api/report/sha256/(Your SHA256)</td>
<td>Uses this url to search using SHA256</td>
<td>GET</td>
</tr>
<tr>
<td>api/report/md5/(Your MD5)</td>
<td>Uses this url to search using MD5</td>
<td>GET</td>
</tr>
</tbody>
</table>

Examples

To get your token using apt:
curl -XPOST http://127.0.0.1:8000/api/get-token/ -d "username=merovingio&password=(pwd)"

To upload a new sample or to check the status of an uploaded sample:
curl -XPOST http://127.0.0.1:8000/api/upload -F file=@sample.exe -H "Authorization: Token d18271a2d52815778cf681707c844667b9d5c255"

To check the status of an uploaded sample using (MD5 / SHA1 / SHA256):
curl http://127.0.0.1:8000/api/report/sha1:584ae71ec6b2b1fd7d2ca40029a78f2aa780a58/ -H "Authorization: Token d18271a2d52815778cf681707c844667b9d5c255"
Merovingio Achievements

- Max. runtime 2 minutes, but the analysis stops when we don’t detect any new behavior.
- We can analyze over 20 samples on the same machine (VM or real).
- To grow, we need to add more RAM memory to allocate more processes or add a new machine to get 20 slots more.
- Very cheap (information for 20 analysis):
  - Only one machine
  - 4Ghz CPU (4 cores) and 4Gb RAM
  - We can stop the analysis when the sample finishes the execution.
Merovingio numbers

• 43,200 samples can be analyzed on each sandbox instance daily

• 864,000 samples using 20 instances on the sandboxie

• Only 1 machine to get this numbers
Questions?