



26th annual **FIRST** conference



BOSTON

M A S S A C H U S E T T S

JUNE 22-27, 2014

Back to the 'root' of Incident Response

Boston Park Plaza Hotel | June 22-27, 2014



Instituto Nacional
de Tecnologías
de la Comunicación

Merovingio: mislead the malware

Juan Carlos Montes – INTECO-CERT



BOSTON



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

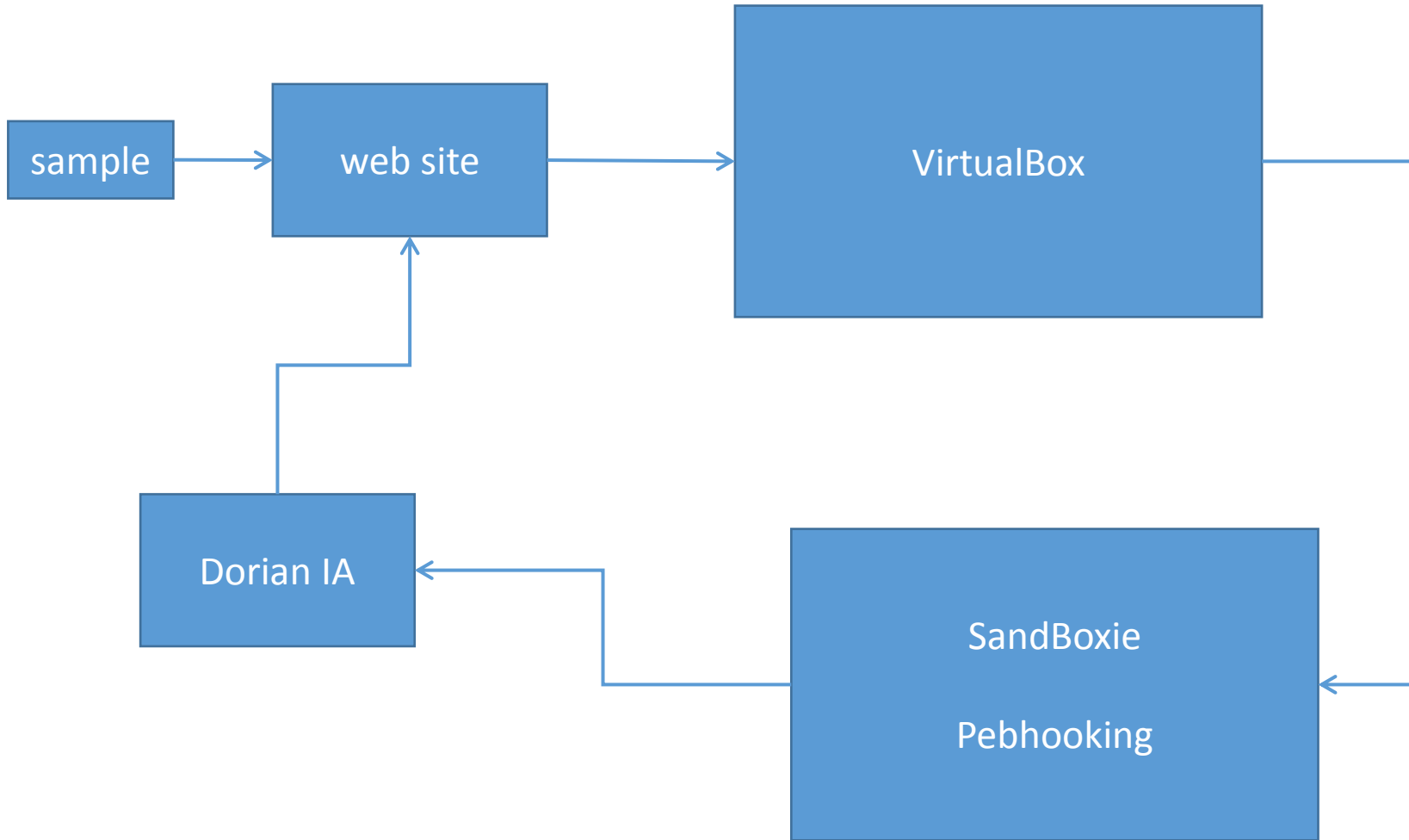
- “Virtual Machine”
- Sandboxie
- Pebhooking
- DorianIA



The screenshot shows a web interface for 'Merovingio'. At the top left, the word 'Merovingio' is written in red. Below it, the word 'Login' is displayed. To the right of the text, there are two input fields: the top one has a person icon and the bottom one has a key icon. Below these fields are two buttons labeled 'Login' and 'Clear'. At the bottom right of the page, there is a small copyright notice: '© INTECO - CERT 2014'.

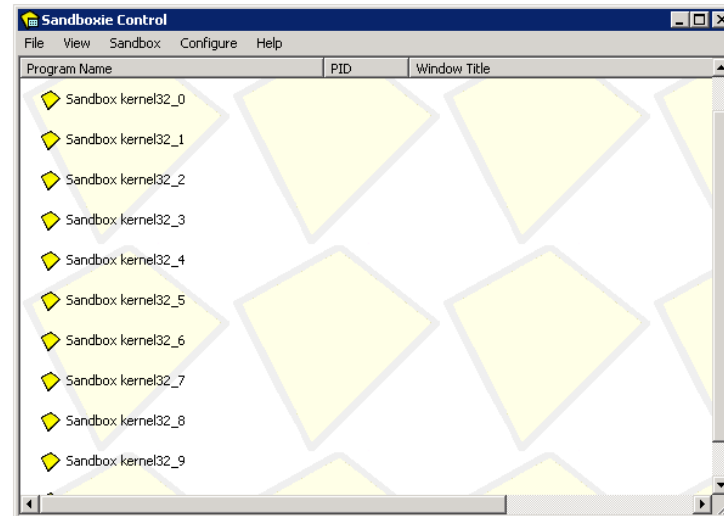
- And... his web site 😊

Merovingio





- 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 that one sample at 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

- `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 | XXXXXXXXXX  
CloseHandle | 0x4C  
CloseHandle | 0x178
```

Block

```
CreateFileW | C:\ikkka.exe | 0x178  
WriteFile | 0x178 | 0x22800 | XXXXXXXXXX  
CloseHandle | 0x178
```


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

The screenshot shows the Merovingio web application interface. At the top left is the 'Merovingio' logo. To its right are navigation links: 'Home' (with a house icon), 'History' (with a list icon), 'Settings' (with a gear icon), and 'Logout' (with a door icon). The main content area is titled 'New analisys' and contains a file upload form. The form has a large grey input field and a 'Choose files' button with a folder icon. Below the input field is a blue 'Analyze' button. At the bottom of the page, it says 'Logged in as admin' and '© INTECO - CERT 2014'.

Merovingio Achievements

- Max. runtime 2 minutes, but the analysis stop when we don't detect any new behavior
- We can analyze over 20 samples on the same machine (VM or real)
- To grown we need add more RAM memory to allocate more process 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 finish 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?

