NoAH Developments

Andreas Bunten / Jan Kohlrausch

DFN-CERT Services GmbH
[bunten|kohlrausch]@dfn-cert.de
NoAH Project: Introduction

- EU project of the 6th framework
  - Leader: FORTH
  - Start April 2005
  - End Sep 2008
NoAH Project: Overall aims

- Set-up of a honeynet
- Hybrid architecture
  - Cooperation of:
    - low-interaction sensors
    - high-interaction (Argos-sensors)
- Generation of attack signatures
NoAH Project: Argos-Sensor

- High-interaction honeypot
  - Based on QEMU emulator
- Instrumented for dynamic taint analysis on network data
  - Designed to reliably detect buffer overflow and related attacks
NoAH Project: Argos alert

```
 Net tracker data: YES  Attack-packet available?

<table>
<thead>
<tr>
<th>VERSION</th>
<th>ARCH</th>
<th>TYPE</th>
<th>Type of alert</th>
<th>TIMESTAMP</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x02</td>
<td>i386</td>
<td>RET</td>
<td></td>
<td>1194963783</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FAX</th>
<th>ECX</th>
<th>EDX</th>
<th>EBX</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00000000</td>
<td>0x000acdd0</td>
<td>0x00085aca</td>
<td>0x005bfed18</td>
</tr>
<tr>
<td>(0x00000000)</td>
<td>(0x00000000)</td>
<td>(0x00000000)</td>
<td>(0x00000000)</td>
</tr>
<tr>
<td>[637]</td>
<td>[637]</td>
<td>[637]</td>
<td>[637]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ESP</th>
<th>EBP</th>
<th>ESI</th>
<th>EDI</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x005bf7bc</td>
<td>0x19eb10eb</td>
<td>0x000bb310</td>
<td>0x000bc7fc</td>
</tr>
<tr>
<td>(0x00000000)</td>
<td>(0x067957ac)</td>
<td>(0x00000000)</td>
<td>(0x00000000)</td>
</tr>
<tr>
<td>[637]</td>
<td>[669]</td>
<td>[637]</td>
<td>[637]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EIP</th>
<th>EFLAGS</th>
<th>Faulty EIP</th>
<th>Address of RET assembly command</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x0018759f</td>
<td>0x00000202</td>
<td>0x75079a0d</td>
<td></td>
</tr>
<tr>
<td>(0x067957b0)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[673]</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Program counter

<table>
<thead>
<tr>
<th>BLOCK#</th>
<th>VERSION</th>
<th>TAINTED</th>
<th>SIZE</th>
<th>PADDR</th>
<th>VADDR</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x01</td>
<td>YES</td>
<td>4</td>
<td>0x06732028</td>
<td>0x00080028</td>
</tr>
<tr>
<td>1</td>
<td>0x01</td>
<td>YES</td>
<td>8</td>
<td>0x067b88b8</td>
<td>0x0008db68</td>
</tr>
<tr>
<td>2</td>
<td>0x01</td>
<td>YES</td>
<td>744</td>
<td>0x06d326b8</td>
<td>0x000946b8</td>
</tr>
</tbody>
</table>
```

© 2008 DFN-CERT Services GmbH / NoAH Development
NoAH Project: Current state

- The demonstrator testbed is up

- Two sensors:
  - Windows XP without any SP
    - Vulnerable Apache 1.3.24 webserver
    - A lot of other known vulnerabilities
  - SuSE 9.3
    - ssh server
    - vsftpd FTP server
    - Standard SuSE apache webserver
NoAH Project: Current state

- **Data presentation service online**
  - Based on weasel presentation of Snort alerts
  - Extension for graphical data presentation

- **Two versions**
  - Project internal
  - Version for cooperating sites containing anonymized data
NoAH Project: Presentation

- Alerts in tabular form

![Tabular Alerts Example](https://sundance.dfn-cert.de/noah/weasel004/index.php?action=sidstat&fit... sundance.dfn-cert.de)
**Attacks in graphical form**
NoAH Project: first results

- Very few attacks against SuSE linux
- MS-SQL worm is by far the most frequent attack detected by snort and Argos
- Many attacks exploiting known windows vulnerabilities
  - Not all succeed
  - Corresponding snort alert for each attack
  - However, not all are detected by snort as exploit
- No attacks against vulnerable apache server
NoAH Project: Fun

Initializing...

Loaded {BD96C556-65A3-11D0-983A-00C04FC29E36}

Creating helper objects...

Creating the XMLHTTP object...

Downloading the payload...

Writing the payload to disk...

Executing the payload...

Tempmetasploit.exe

Tempmetasploit.exe has encountered a problem and needs to close. We are sorry for the inconvenience.

If you were in the middle of something, the information you were working on might be lost.

Please tell Microsoft about this problem.
We have created an error report that you can send to us. We will treat this report as confidential and anonymous.

To see what data this error report contains, click here.

Send Error Report  Don't Send
Outlook

- Next steps will extend the demonstrator testbed
- Cooperating sites are welcome!
  - Will be announced on the TF-CSIRT mailing-list
Questions?

Andreas Bunten / Jan Kohlrausch
https://www.dfn-cert.de/
[bunten|kohlrausch]@dfn-cert.de