Detecting the ghost in the browser: Real time detection of drive-by infections

Thijs Kinkhorst    Michael van Kleij

1 July 2009
Nine-Ball hacker attack rolls on

Web ad sales open door to viruses

Microsoft sounds alarm about PDF-attacks

Mass injection, Nine-ball infects more than 40,000 legitimate web sites

Canadian MSN site Sympatico compromised
What is a drive-by infection?

- Legitimate websites are compromised.
- An iFRAME is included which points to a browser exploit.

Example

```html
```
Research question

*Can drive-by infections be discerned from legitimate sessions purely by measuring changes in HTTP traffic patterns and meta data?*

- Enables detection by monitoring the local network.
- Low chance on false positives or false negatives.
Scope

- Detection via network traffic, not on the client machine.
- Not HTTP content inspection, no signature matching.
- Only infections that require no user interaction.
- Just the infection itself, not subsequent behaviour of the malware.
Lab setup and dataset composition

- Infected sites in our dataset are found using www.malwaredomainlist.com and similar.
- Each site was tested in a clean virtual machine using a test protocol.
- Test protocol consists of:
  - Start capture.
  - Visit site, wait 2 minutes.
  - Close browser, wait 2 minutes.
  - Shut down machine.
  - Restore machine to clean state, rotate IP address.
- Capturing both clean sessions and infected sessions.
Analysis

- TCP port numbers.
- Geographical locations.
- Hostnames.
- User agents.
- Invalid POST requests.
- Request URIs.
- Content types.
- Redirection.
## TCP port numbers

<table>
<thead>
<tr>
<th>Port</th>
<th>Clean # of sess.</th>
<th>Clean % of sess.</th>
<th>Infected # of sess.</th>
<th>Infected % of sess.</th>
</tr>
</thead>
<tbody>
<tr>
<td>port 80</td>
<td>39</td>
<td>100%</td>
<td>25</td>
<td>100%</td>
</tr>
<tr>
<td>port 8080</td>
<td>0</td>
<td>0%</td>
<td>10</td>
<td>40%</td>
</tr>
<tr>
<td>port 443</td>
<td>3</td>
<td>8%</td>
<td>2</td>
<td>8%</td>
</tr>
</tbody>
</table>
### User agents

<table>
<thead>
<tr>
<th></th>
<th>Clean sess.</th>
<th>Infected sess.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total number of different User-Agent headers found</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>Average number of unique User-Agent headers per session</td>
<td>1.0</td>
<td>2.5</td>
</tr>
<tr>
<td>Average number of requests with non-original User-Agent per session</td>
<td>0.2</td>
<td>6.1</td>
</tr>
</tbody>
</table>
Redirection
Detection method

- Scoring like SpamAssassin.
- Combine inconclusive information into high-confidence verdict.
- Flexible and expandable

\[
\begin{align*}
\text{score} & \leftarrow 0 \\
\text{firstrequest} & \leftarrow \text{front}(\text{capture}) \\
\text{for all } \text{rule} \in \text{ruleset } \text{do} \\
& \quad \text{score} \leftarrow \text{score} + \min ( \text{rule}(\text{capture}, \text{firstrequest}), 4.0 ) \\
\text{end for} \\
\text{return } \text{score} \geq 5.0
\end{align*}
\]
TCP port numbers

**Rule 1** Detecting ‘bad’ ports

```plaintext
function Rule (capture, firstreq) : s
for all request ∈ capture do
    if request.port ∉ \{80,443\} ∧ request.port ≠ firstreq.port then
        return 2.0
    end if
end for
return 0
end function
```
User Agents

Rule 6 Detecting ‘bad’ user agents

```python
function Rule (capture, firstreq) : s
    s ← 0
    for all request ∈ capture do
        if request.useragent ∉ α ∧ request.useragent ≠ firstreq.useragent then
            s ← s + 0.4
        end if
    end for
    return s
end function
```

α: whitelist of special user agents, like Adobe Updater.
Redirection Trees

**Rule 10** Analysing redirection trees

```plaintext
function Rule (capture, firstreq) : s
    T ← BuildRedirectionTree (capture)
    return min ( max ( 0, height(T) − 2 ), 2.0 )
end function
```

\[
\text{height}(T) \leq 2 \Rightarrow 0.0
\]
\[
\text{height}(T) = 3 \Rightarrow 1.0
\]
\[
\text{height}(T) \geq 4 \Rightarrow 2.0
\]
Validation

- Collected second, separate dataset for testing usefulness.
- Consists of 20 legitimate and 15 infected captures.
- Apply our ruleset to this new data.

- True-negative rate: 14 out of 15 (93%)
- False-positive rate: 0 out of 20 (0%)
Validation: Infected Sessions

<table>
<thead>
<tr>
<th>rule</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>∑</th>
</tr>
</thead>
<tbody>
<tr>
<td>session 1</td>
<td>2.0</td>
<td>2.0</td>
<td>1.0</td>
<td>0.4</td>
<td>2.0</td>
<td>2.0</td>
<td>0.4</td>
<td></td>
<td></td>
<td></td>
<td>9.8</td>
</tr>
<tr>
<td>session 2</td>
<td>2.0</td>
<td>2.0</td>
<td>1.5</td>
<td>1.0</td>
<td>2.0</td>
<td>0.8</td>
<td>2.0</td>
<td>3.0</td>
<td>0.4</td>
<td></td>
<td>14.7</td>
</tr>
<tr>
<td>session 3</td>
<td>1.5</td>
<td>1.0</td>
<td>4.0</td>
<td></td>
<td>1.0</td>
<td>1.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8.7</td>
</tr>
<tr>
<td>session 4</td>
<td>1.5</td>
<td>2.0</td>
<td>0.4</td>
<td></td>
<td></td>
<td></td>
<td>1.6</td>
<td>2.0</td>
<td></td>
<td></td>
<td>7.5</td>
</tr>
<tr>
<td>session 5</td>
<td>1.5</td>
<td>2.0</td>
<td>0.8</td>
<td></td>
<td></td>
<td></td>
<td>1.8</td>
<td>2.0</td>
<td></td>
<td></td>
<td>8.1</td>
</tr>
<tr>
<td>session 6</td>
<td>1.5</td>
<td>2.0</td>
<td>0.8</td>
<td></td>
<td></td>
<td></td>
<td>0.4</td>
<td>2.0</td>
<td></td>
<td></td>
<td>6.7</td>
</tr>
<tr>
<td>session 7</td>
<td>2.0</td>
<td>2.0</td>
<td>1.0</td>
<td></td>
<td></td>
<td></td>
<td>1.0</td>
<td>0.4</td>
<td></td>
<td></td>
<td>6.4</td>
</tr>
<tr>
<td>session 8</td>
<td>1.5</td>
<td>2.0</td>
<td>0.4</td>
<td></td>
<td></td>
<td></td>
<td>2.2</td>
<td>2.0</td>
<td></td>
<td></td>
<td>8.1</td>
</tr>
<tr>
<td>session 9</td>
<td>2.0</td>
<td>2.0</td>
<td>1.0</td>
<td></td>
<td></td>
<td>2.0</td>
<td>2.0</td>
<td>0.4</td>
<td></td>
<td></td>
<td>9.4</td>
</tr>
<tr>
<td>session 10</td>
<td>2.0</td>
<td>2.0</td>
<td>1.0</td>
<td></td>
<td></td>
<td>2.0</td>
<td>3.0</td>
<td>0.4</td>
<td></td>
<td></td>
<td>10.4</td>
</tr>
<tr>
<td>session 11</td>
<td>1.5</td>
<td>2.0</td>
<td>0.8</td>
<td></td>
<td></td>
<td></td>
<td>1.0</td>
<td>2.0</td>
<td></td>
<td></td>
<td>7.3</td>
</tr>
<tr>
<td>session 12</td>
<td>1.5</td>
<td>2.0</td>
<td>0.8</td>
<td></td>
<td></td>
<td></td>
<td>2.0</td>
<td>2.0</td>
<td></td>
<td></td>
<td>8.3</td>
</tr>
<tr>
<td>session 13</td>
<td>2.0</td>
<td>1.5</td>
<td>1.0</td>
<td>2.0</td>
<td>1.2</td>
<td>1.0</td>
<td>0.2</td>
<td></td>
<td></td>
<td></td>
<td>8.9</td>
</tr>
<tr>
<td>session 14</td>
<td>1.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.2</td>
<td></td>
<td></td>
<td></td>
<td>1.7</td>
</tr>
<tr>
<td>session 15</td>
<td>2.0</td>
<td>1.5</td>
<td>2.0</td>
<td>1.6</td>
<td>1.0</td>
<td>1.0</td>
<td>1.0</td>
<td></td>
<td></td>
<td></td>
<td>9.1</td>
</tr>
</tbody>
</table>
## Validation: Clean Sessions

<table>
<thead>
<tr>
<th>rule</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>∑</th>
</tr>
</thead>
<tbody>
<tr>
<td>session 1</td>
<td></td>
<td></td>
<td>1.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.5</td>
</tr>
<tr>
<td>session 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 3</td>
<td></td>
<td></td>
<td>1.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.5</td>
</tr>
<tr>
<td>session 4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 8</td>
<td></td>
<td></td>
<td>1.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.5</td>
</tr>
<tr>
<td>session 9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2.0</td>
</tr>
<tr>
<td>session 15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.0</td>
</tr>
<tr>
<td>session 19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0.0</td>
</tr>
<tr>
<td>session 20</td>
<td></td>
<td></td>
<td>1.5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.5</td>
</tr>
</tbody>
</table>

T. Kinkhorst, M. van Kleij: Detecting the ghost in the browser
Conclusion

*Can drive-by infections be discerned from legitimate sessions purely by measuring changes in HTTP traffic patterns and meta data?*

Yes, it is possible.

Focus points:
- Scoring and rules need more real-life improvement.
- Identification of a session may be problematic.
Thank You

Questions?