Security Web Scanners

- Normalized URL: http://www.yahoo.com/
- Detection ratio: 0 / 38
- Analysis date: 2013-07-02 12:15:47 UTC (0 minutes ago)
- File scan: The URL response content could not be retrieved or it is some text format (HTML, XML, CSV, TXT, etc.), hence, it was not enqueued for antivirus scanning.

<table>
<thead>
<tr>
<th>URL Scanner</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMINUSLabs</td>
<td>Clean site</td>
</tr>
<tr>
<td>AlienVault</td>
<td>Clean site</td>
</tr>
<tr>
<td>Avira</td>
<td>Clean site</td>
</tr>
<tr>
<td>BitDefender</td>
<td>Clean site</td>
</tr>
<tr>
<td>C-SIRT</td>
<td>Clean site</td>
</tr>
<tr>
<td>CLEAN MX</td>
<td>Clean site</td>
</tr>
</tbody>
</table>
What is RDI?

Reflected DOM Injection

Web Service

User

Malicious

Legit

Our Website
A Recipe for Disaster

- 1 simple web page
- 1 trustworthy web utility
- 1 script that behaves differently within a certain context
- 2 cups of funny cat pictures
Yahoo Cache
What Just Happened!?
Let’s Take it a Step Further

Google Translate
Go back in time (10 minutes ago)

- Producing a malicious URL “hosted” on Google

  ![Google Translate](http://handei.ueuo.com/tran.html)

- We will be able to access it directly without the interface:
  
What happens behind the scenes

Malicious

User → Google Translate → Malicious → Our Website
After the text is translated, the malicious code is generated, decrypted and executed.
Reflected DOM Injection

- RDI is a technique
- Context makes the difference
- Very hard to detect
- RDI is awesome!
VirusTotal / Wepawet?

![VirusTotal Screen](image)

- **Detection ratio:** 1 / 39
- **File scan:** The URL response content could not be retrieved or it is some text format (HTML, XML, CSV, TXT, etc.), hence, it was not enqueued for antivirus scanning.

<table>
<thead>
<tr>
<th>URL Scanner</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMINUSLabs</td>
<td>Clean site</td>
</tr>
<tr>
<td>AlienVault</td>
<td>Clean site</td>
</tr>
<tr>
<td>Anti- AVL</td>
<td>Clean site</td>
</tr>
<tr>
<td>Avira</td>
<td>Clean site</td>
</tr>
<tr>
<td>BitDefender</td>
<td>Clean site</td>
</tr>
<tr>
<td>C-SIRT</td>
<td>Clean site</td>
</tr>
<tr>
<td>CLEAN MX</td>
<td>Clean site</td>
</tr>
<tr>
<td>Comodo Site Inspector</td>
<td>Clean site</td>
</tr>
<tr>
<td>CyberCrime</td>
<td>Clean site</td>
</tr>
</tbody>
</table>

**Sucuri SiteCheck:** Malicious site
Thank You!

Q & A

Daniel Chechik: 
[mailto:dchechik@trustwave.com dchechik@trustwave.com] @danielchechik

Anat (Fox) Davidi: 
[mailto:adavidi@trustwave.com adavidi@trustwave.com] @afoxdavidi
More Cats!