UTILIZING POPULAR WEBSITES FOR MALICIOUS PURPOSES USING RDI

Daniel Chechik, Anat (Fox) Davidi
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>
<tr>
<td>Comodo Site Inspector</td>
<td>Suspicious site</td>
</tr>
<tr>
<td>CyberCrime</td>
<td>Unrated site</td>
</tr>
<tr>
<td>Dr. Web</td>
<td>Clean site</td>
</tr>
<tr>
<td>ESET</td>
<td>Clean site</td>
</tr>
<tr>
<td>Fortinet</td>
<td>Unrated site</td>
</tr>
<tr>
<td>G-Data</td>
<td>Clean site</td>
</tr>
</tbody>
</table>
What is RDI?

RDI

Science and technology

- Recover Data Interface - Part (EN 50255) of the DAB Digital Audio Broadcasting standard
- Reference Daily Intake or Recommended Daily Intake, a quantity of recommended nutrient intake
- Relationship Development Intervention, a treatment for autism
- Relative dose intensity, a term used in describing chemotherapy; for example with Cyclophosphamide, met
- Resistance Database Initiative, a not-for-profit HIV research organisation
- Respiratory disturbance index, a tool for measuring frequency of breathing related sleep disturbances
- RDI register, a 64-bit processor register of x86 CPUs

Organisations

- Réseau de l'information, a Canadian French language news channel owned by Radio-Canada
- RDI Video Systems, a video game company
- Response Dynamics, a conservative direct marketing firm
- Rural Development Institute, Canadian research center

Other

- Regimental Distinctive Insignia, US Army regimental insignia
- Royal Designers for Industry, a British honour bestowed on leading designers by the Royal Society of Arts
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
function booyah() {
  var x = document.getElementById("wakadiv").innerHTML;
  var y = document.getElementsByTagName("span")[1].innerHTML;
  var key = 0;
  for (var i = 0; i < y.length; i++) {
    key += y.charCodeAt(i);
  }
}

<base href="http://www.testwpekfwoekfpwoekfpwoefk.com/"/>
<meta http-equiv="content-type" content="text/html; charset=utf-8"/>

-- Banner:Start -->
<style type="text/css">
.b_cpb { color: black; font: normal normal normal small normal arial,sans-serif } 
.b_cpb a { color: blue; text-decoration: underline; font-weight: normal }
</style>

...reached the cached page

...content:Start -->
<div style="display:none;">
  The search results. The page loaded (without the
</div>

...not responsible for the

...Banner:End -->
<div style="display:none;">
Let’s Take it a Step Further

Google Translate
Go back in time (10 minutes ago)

- Producing a malicious URL “hosted” on Google


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

Malicious
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?

Normalized URL: http://translate.google.com/translate?

Detection ratio: 1/39

Date: 2013-07-11 10:39:31 UTC (2 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.

Analysis:

Sucuri SiteCheck: Malicious site
Thank You!

Q & A

Daniel Chechik:

dchechik@trustwave.com @danielchechik

Anat (Fox) Davidi:

adavidi@trustwave.com @afoxdavidi
More Cats!