

Zararlı JavaScript Avı

written by Mert SARICA | 1 April 2016

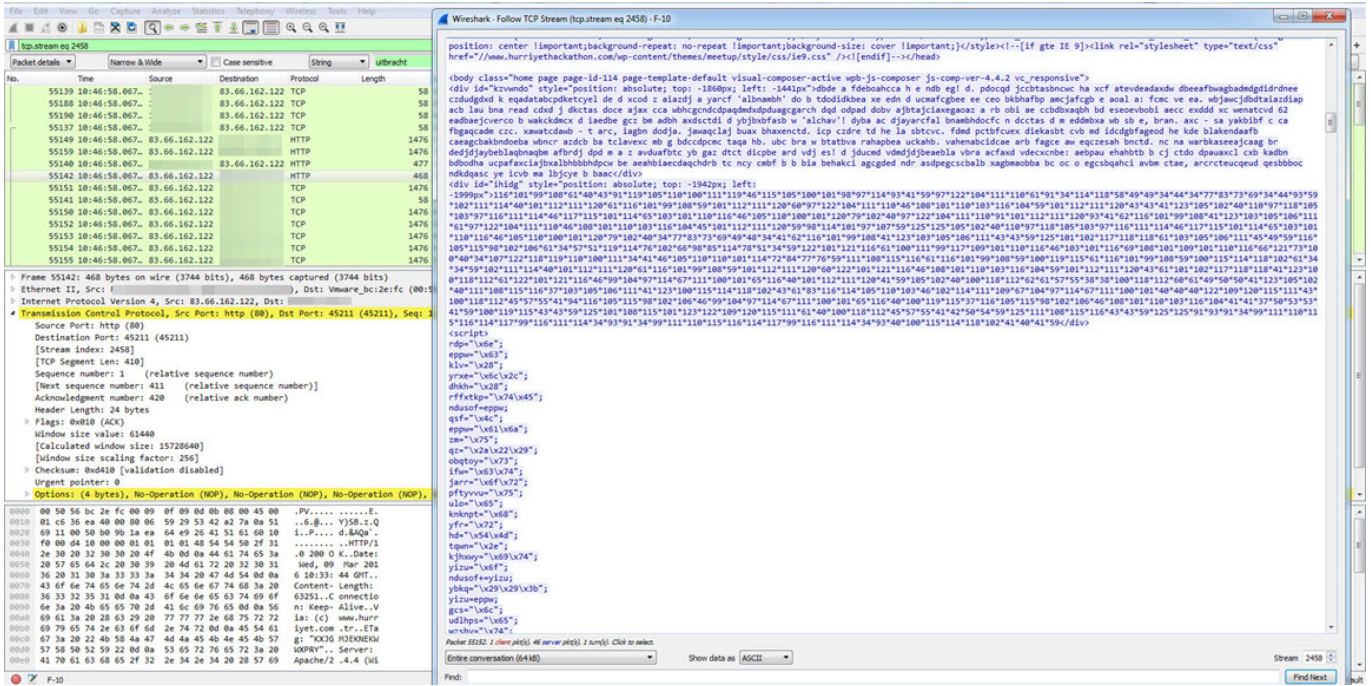
Kum havuzu (sandbox) analizi yapan teknolojiler/cihazlar, kurumlara doğrudan ya da dolaylı olarak yapılan siber saldırıları tespit etme, gerekli önlemleri alma veya aldırma noktasında oldukça önemli bir role sahiptir. Bu cihazlarda ortaya çıkan alarmlar kurumsal SOME'ler tarafından incelendiğinde, kimi 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		# Visits		Total URLs		First URL at		Last URL at				
uitbracht.kateandoliverswedding.co.uk/topic/18572-indivisible-arri-ver-existences-far-off-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-arri-ver-existences-far-off-prepositions-sunburn-crushing-hittable/				03/09/16 12:46:57		text/html						
uitbracht.kateandoliverswedding.co.uk/?v=Tx7Tb6d=Qpvl7x2LV58l=GC72Vks0V08b=K3baa7T4u8,ic=5u1Vx6e=7u850xc				03/09/16 12:46:57		application/x-shockwave-flash						
uitbracht.kateandoliverswedding.co.uk/?v=ixlK0EdgK8c=Y6Q98a=8l=1L1QNd5=8t=3H4T8f=8n=uk3MSa=RP8m=IfcPndTg8b=8d=Qxnlbu				03/09/16 12:46:57		text/html						
uitbracht.kateandoliverswedding.co.uk/?p=8n=vvv8f=zbW08t=FBC3Xu0_8h=5M38v=A3lD2Sc27vvyat_T3P86a_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)



Yukarda 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, çalıştırsın 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 koduna 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.



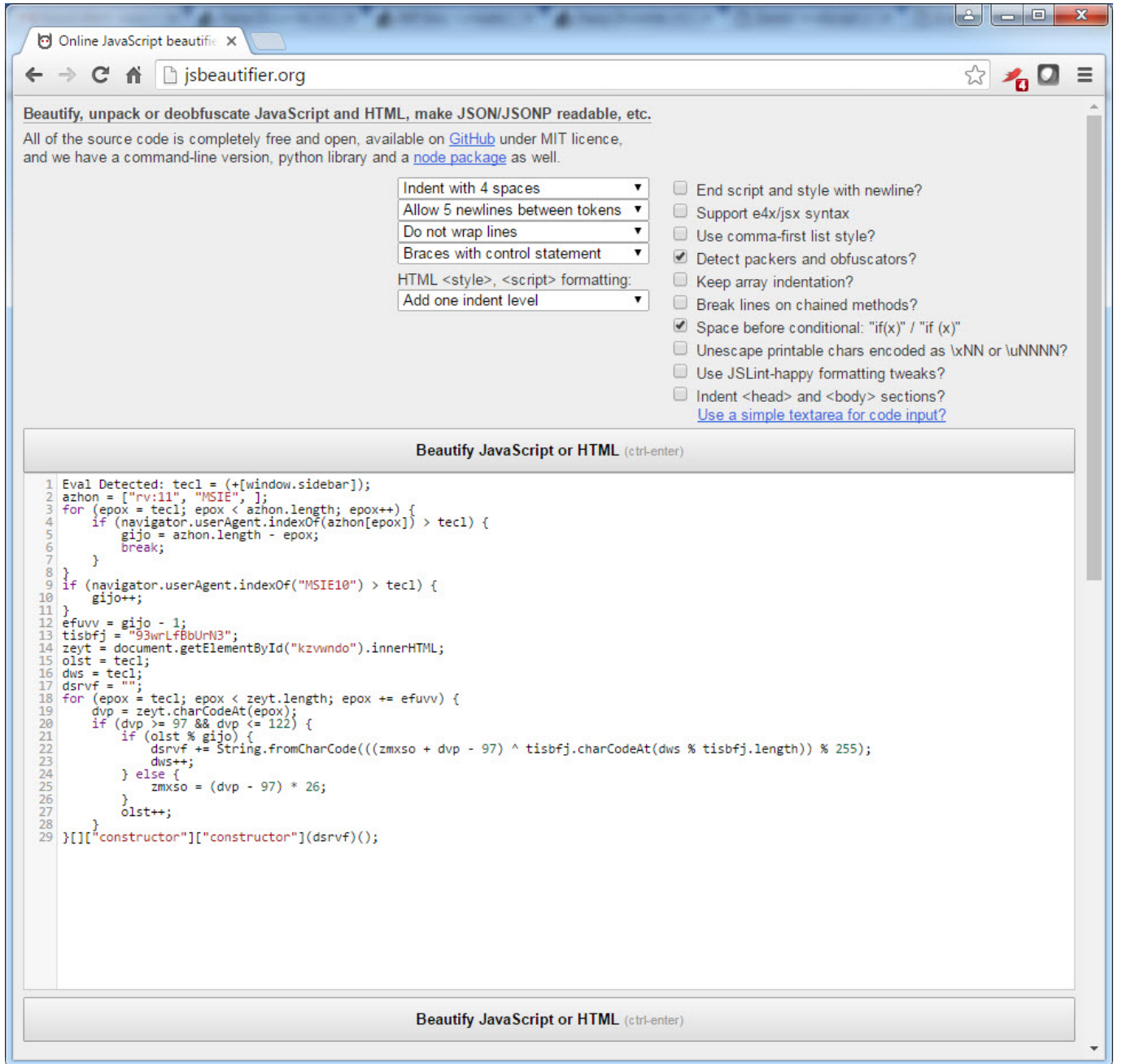
remnux@remnux: ~/Desktop/hurriyethackathon



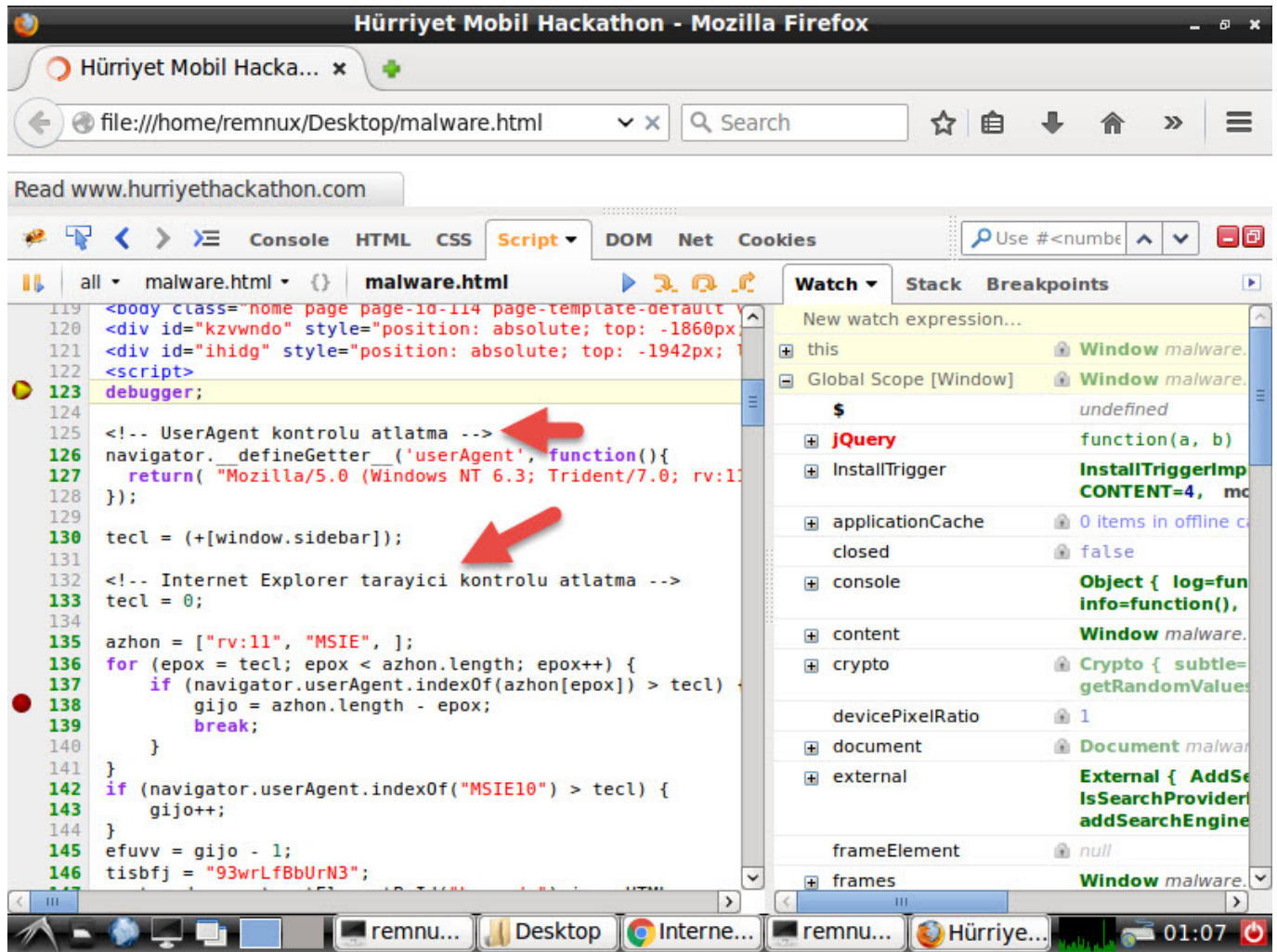
```
remnux@remnux:~/Desktop/hurriyethackathon$ python eval-finder.py hurriyethackathon.pcap
=====
JavaScript Eval Finder v1.0 [http://www.mertsarica.com]
=====
[*] Loading PCAP file...
[*] Loading sessions...
[*] JavaScript detected
[*] Writing html file hurriyethackathon.pcap-1458229564.html to javascripts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

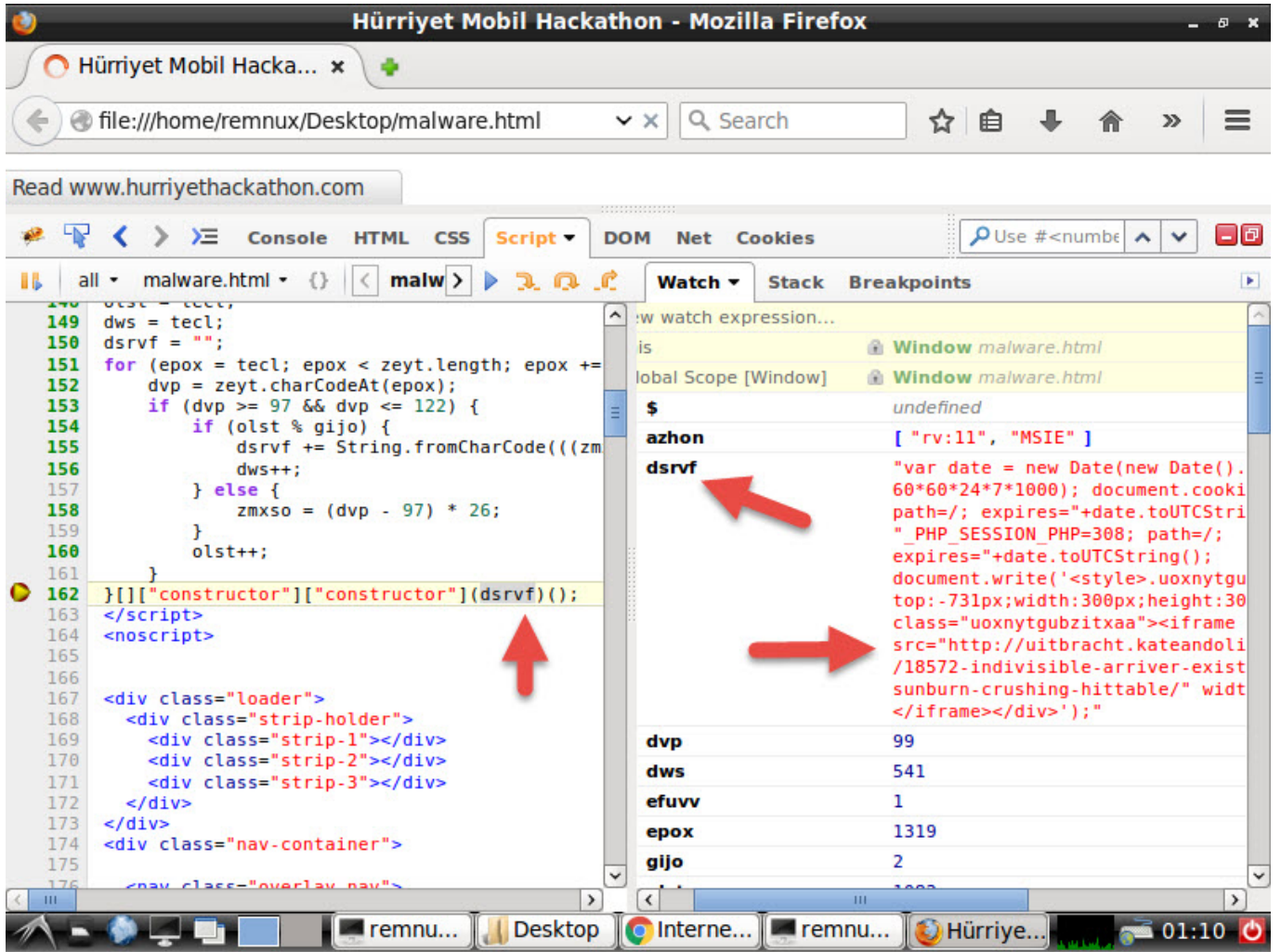
[*] Suspicious file: hurriyethackathon.pcap-1458229564.html
[*] eval() Detected: tecl=(+[window.sidebar]);azhon=["rv:11","MSIE",];for(epox=tecl;epox<
l){gijo=azhon.length-epox;break;}}if(navigator.userAgent.indexOf("MSIE10")>tecl){gijo++;}
wndo").innerHTML;olst=tecl;dws=tecl;dsrvf="";for(epox=tecl;epox<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$
```



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.





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 ;)