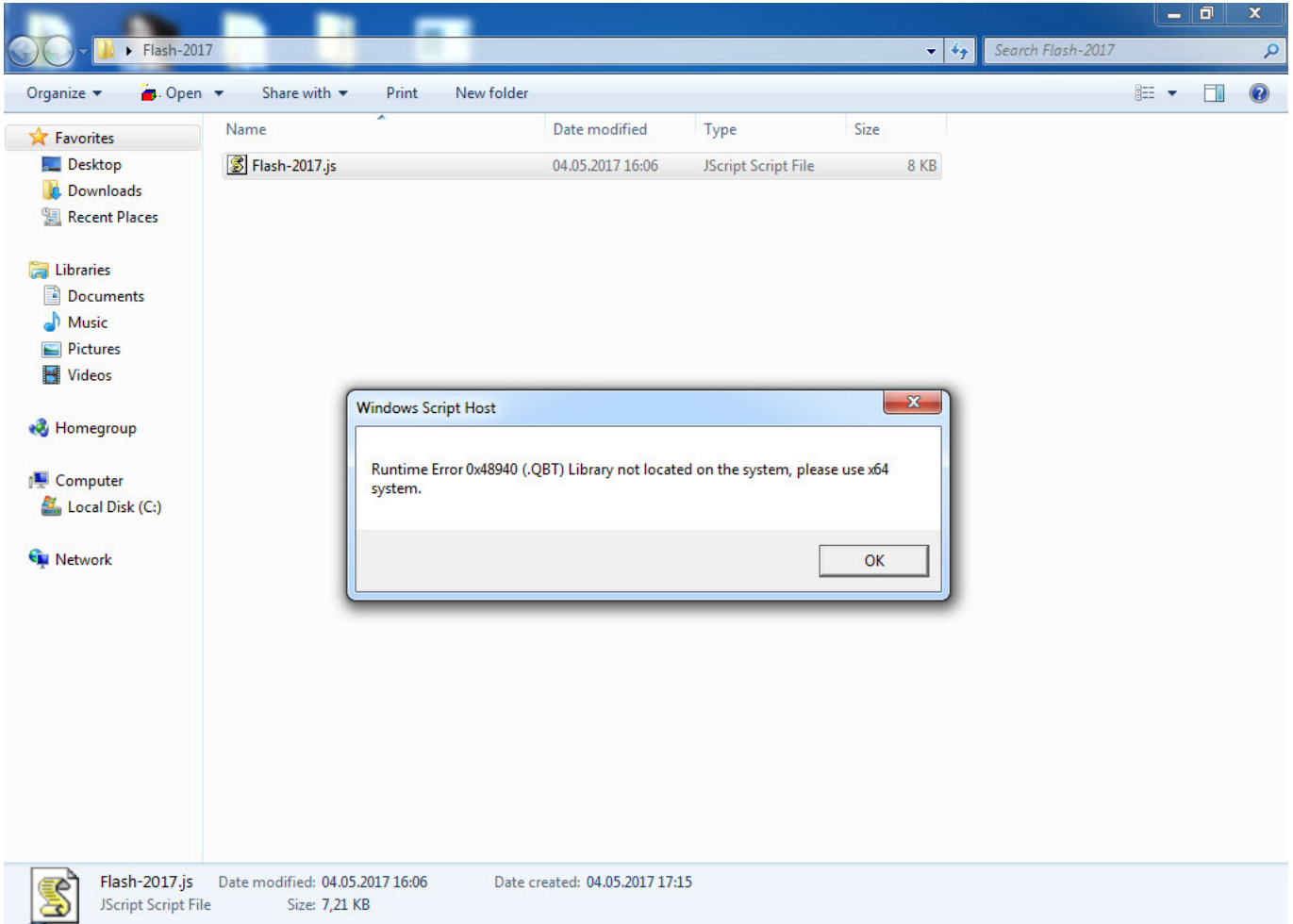
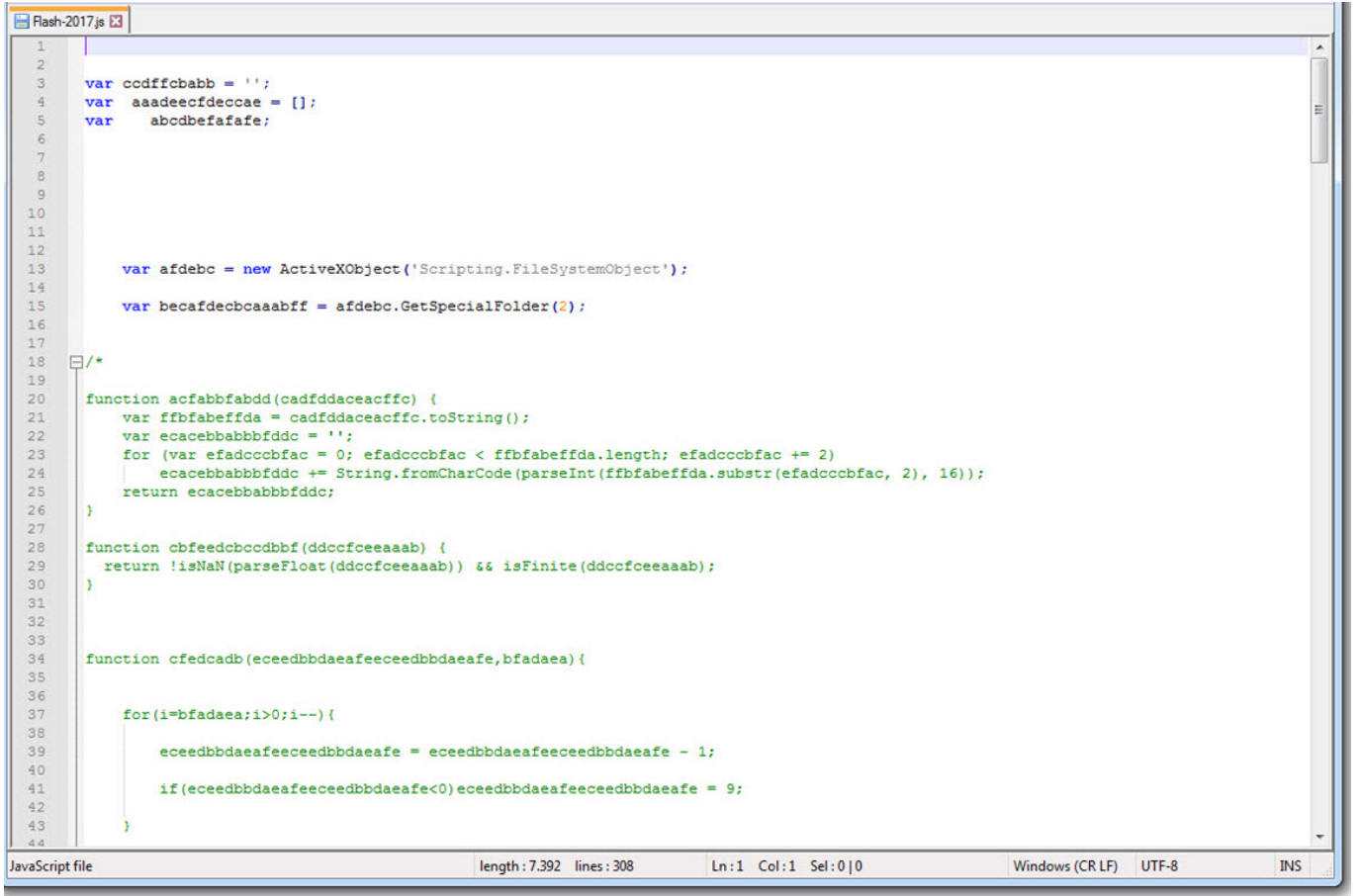


(W/C)script Hata Ayıklaması

written by Mert SARICA | 1 January 2018

Okuyanlarınızın Man In The Proxy blog yazıma konu olan bir internet bankacılığı zararlı yazılımını hedef sisteme indirmek ve çalıştırmak amacıyla zararlı bir JScript dosyası (Flash-2017.js) kullanıldığını anımsayacaklardır. O yazıda okunaklı olmayan (encoded) bu JScript dosyasının Zararlı JavaScript Analizi başlıklı yazımda olduğu gibi internet tarayıcısı ile basit bir şekilde analiz edilemediğine yer vermiştim. Bunun sebebi ise JScript dosyasının çalışma esnasında ActiveX ve WScript kullanımına ihtiyaç duymasıydı. (“WScript is not defined”, “ActiveXObject is not defined”) Internet tarayıcısı ile Jscript dosyasının analiz edilemediği kimi durumlarda hem Visual Studio’dan hem de ücretsiz sürümü olan Visual Studio Express’ten faydalanabilirsiniz.

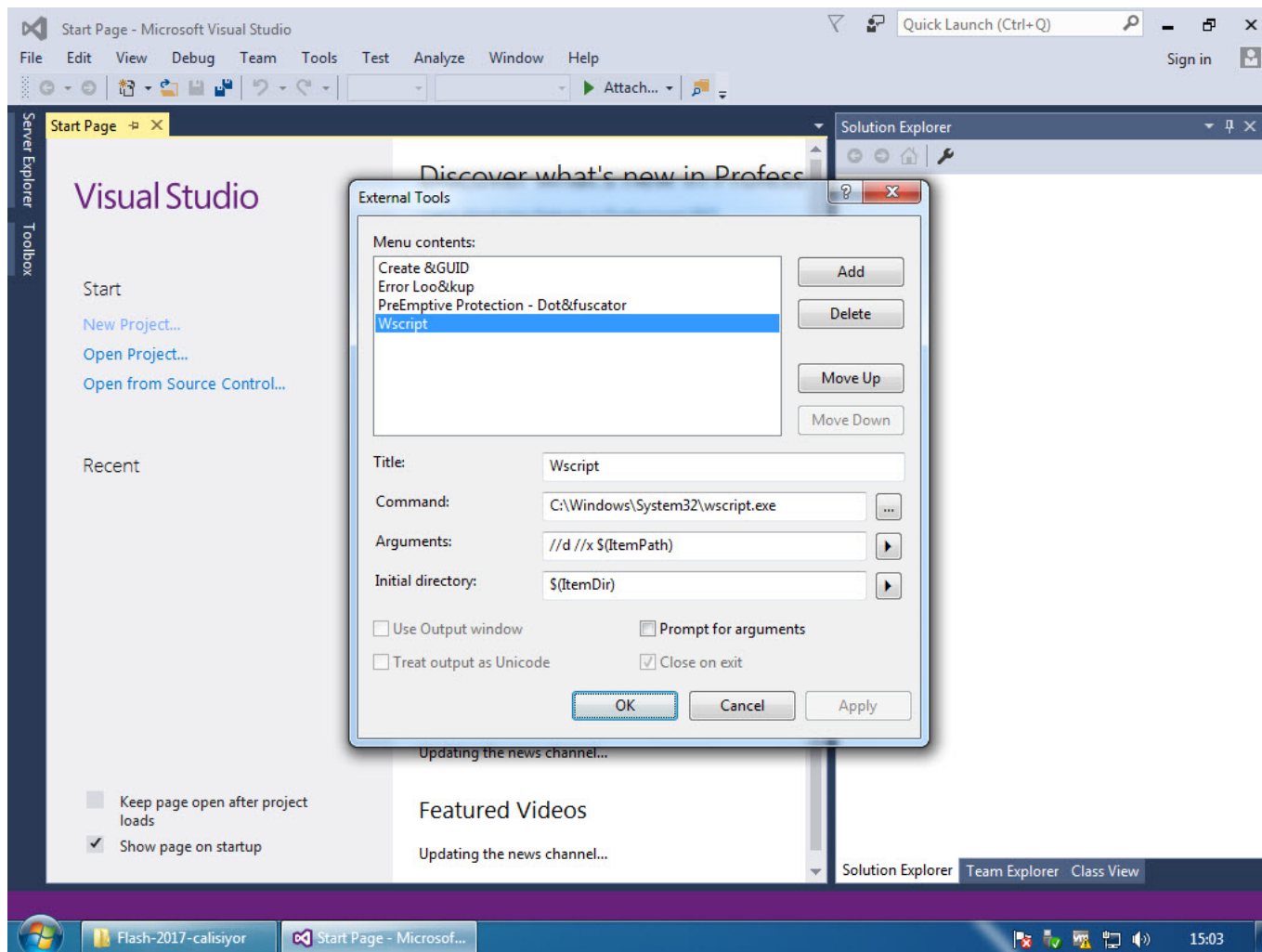


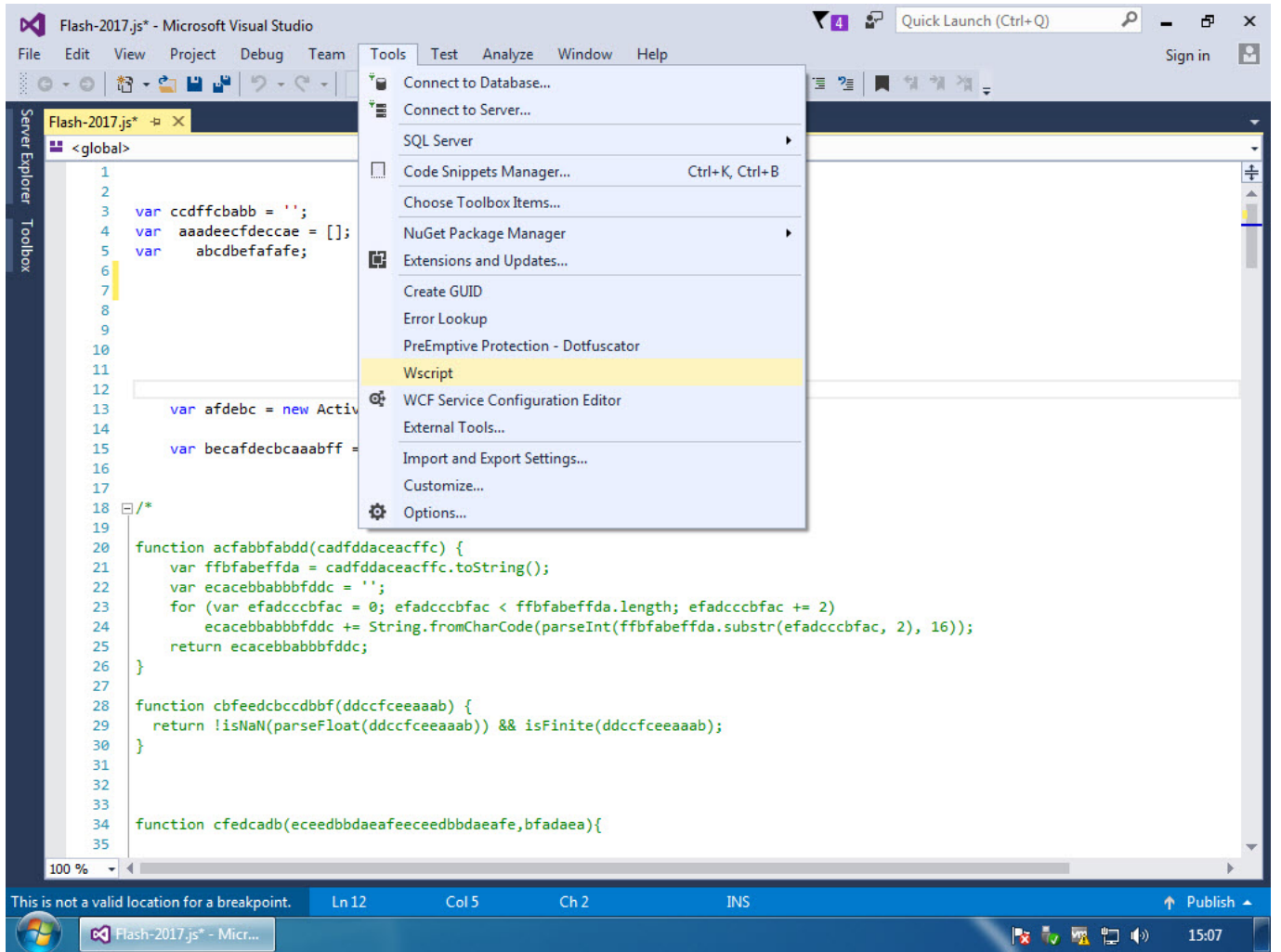
A screenshot of a code editor window titled 'Flash-2017.js'. The editor displays a JavaScript file with obfuscated code. The code includes variable declarations, a call to 'ActiveXObject', and several functions designed to decode the obfuscated strings. The status bar at the bottom indicates the file is a 'JavaScript file', has a length of 7,392, 308 lines, and is using 'Windows (CR LF)' encoding with 'UTF-8' character set. The editor interface includes a line number column on the left and a scrollbar on the right.

```
1
2
3 var ccdffcbabb = '';
4 var aaadeecfdeccae = [];
5 var abcdbeafafe;
6
7
8
9
10
11
12
13 var afdebc = new ActiveXObject('Scripting.FileSystemObject');
14
15 var becafedecbcaaabff = afdebc.GetSpecialFolder(2);
16
17
18 /*
19
20 function acfabbbabdd(cadfdaceacffc) {
21     var ffbfabeffda = cadfdaceacffc.toString();
22     var ecacebbabbbfddc = '';
23     for (var efadcccbfac = 0; efadcccbfac < ffbfabeffda.length; efadcccbfac += 2)
24         ecacebbabbbfddc += String.fromCharCode(parseInt(ffbabeffda.substr(efadcccbfac, 2), 16));
25     return ecacebbabbbfddc;
26 }
27
28 function cbfeedcbccdbbf(ddccfceeaaab) {
29     return !isNaN(parseFloat(ddccfceeaaab)) && isFinite(ddccfceeaaab);
30 }
31
32
33
34 function cfedcadb(eceedbbdaaeafeeceedbbdaaeafe,bfadaea) {
35
36     for(i=bfadaea;i>0;i--){
37
38         eceedbbdaaeafeeceedbbdaaeafe = eceedbbdaaeafeeceedbbdaaeafe - 1;
39
40         if(eceedbbdaaeafeeceedbbdaaeafe<0)eceedbbdaaeafeeceedbbdaaeafe = 9;
41
42     }
43
44 }
```

Wikipedia'ya göre Microsoft Windows Script Host (WSH) (eski adıyla Windows Scripting Host), Microsoft Windows işletim sistemine özellik açısından BATCH dosyalarına kıyasla çok daha fazlasını vadeden bir betik otomasyon teknolojisi. Birden fazla betik (JScript, VBScript) dosyasını desteklemesi en önemli artılarından birisidir. Not olarak VBS hata ayıklaması için ayrıca VbsEdit isimli araçtan da faydalanabileceğiniz yeri gelmişken söyleyeyim.

Bu gibi durumlarda JScript dosyasını hızlıca analiz edebilmek için ilk olarak Visual Studio'da, Tools -> External Tools menüsü altında Microsoft tarafından belirtilen hata ayıklama parametrelerini tanımlamalısınız. Ardından analiz etmek istediğiniz JScript dosyasını Visual Studio'da açtıktan sonra Tools menüsü altından daha önce tanımladığınız Wscript'i seçerek JScript dosyasını kolayca analiz etmeye başlayabilirsiniz.





Yazıma konu olan Flash-2017.js isimli JScript dosyasını adım adım hata ayıklama ile analiz etmeye başladığımızda, kodun yorum satırlarının (comment) başındaki /* ve */ karakterleri sildiğini görebiliyoruz.

wsript (Debugging) - Microsoft Visual Studio

File Edit View Project Build Debug Team Tools Test Analyze Window Help

Process: [2120] wsript.exe Lifecycle Events Thread: [2068] Thread 2068

Flash-2017.js [dynamic]

```

1
2
3 var ccdffcbabb = '';
4 var aaadeecfdeccae = [];
5 var abcdbefafafe;
6
7
8
9
10
11
12
13 var afdebc = new ActiveXObject('Scripting.FileSystemObject');
14
15 var becafddecbaaabff = afdebc.GetSpecialFolder(2);
16
17
18 /*
19
20 function acfabbbabdd(cadfddeaceaffc) {
21     var ffbfabeffda = cadfddeaceaffc.toString();

```

100 %

Locals

Name	Value	Type
this	{...}	Object
WScript	{...}	Object
WSH	{...}	Object
faabeaddabecfffb	{...}	Object
ccdffcbabb	undefined	Undefined
aaadeecfdeccae	undefined	Undefined
abcdbefafafe	undefined	Undefined
afdebc	undefined	Undefined

Autos Locals Watch1

Call Stack

Name	Lang
JScript global code [Flash-2017.js] Line 3	Script

Call Stack Breakpoints Exception Settin... Command Win... Immediate Win... Output

wsript (Debugging) - Microsoft Visual Studio

File Edit View Project Build Debug Team Tools Test Analyze Window Help

Process: [2120] wsript.exe Lifecycle Events Thread: [2068] Thread 2068

eval code [dynamic]

```

628
629 var afdebc = new ActiveXObject('Scripting.FileSystemObject');
630
631 var becafddecbaaabff = afdebc.GetSpecialFolder(2);
632
633
634 /*
635
636 function acfabbbabdd(cadfddeaceaffc) {
637     var ffbfabeffda = cadfddeaceaffc.toString();
638     var eacebbabbbfddc = '';
639     for (var efadccbfac = 0; efadccbfac < ffbfabeffda.length; efadccbfac += 2)
640         eacebbabbbfddc += String.fromCharCode(parseInt(ffbfabeffda.substr(efadccbfac, 2), 16));
641     return eacebbabbbfddc;
642 }
643
644 function cbfeedcbccdbbf(ddccfceeaaab) {
645     return !isNaN(parseFloat(ddccfceeaaab)) && isFinite(ddccfceeaaab);
646 }
647
648

```

100 %

Locals

Name	Value	Type
abcdbefafafe	undefined	Undefined
afdebc	{...}	IFileSyste
becafdecbaaabff	{...}	IFolder
fcaebcfefce	5	Number
dcbecdebfedea	true	Boolean
cebcddffebafddbcdf	{...}	ITextStre
ebdfddceccdc	"\\n\\n\\nvar ccdffcbabb = '';\\n\\nvar aaadeecfdeccae = [];\\n\\nvar abcdbefafafe = '';	String
acfabbbabdd	function	Object

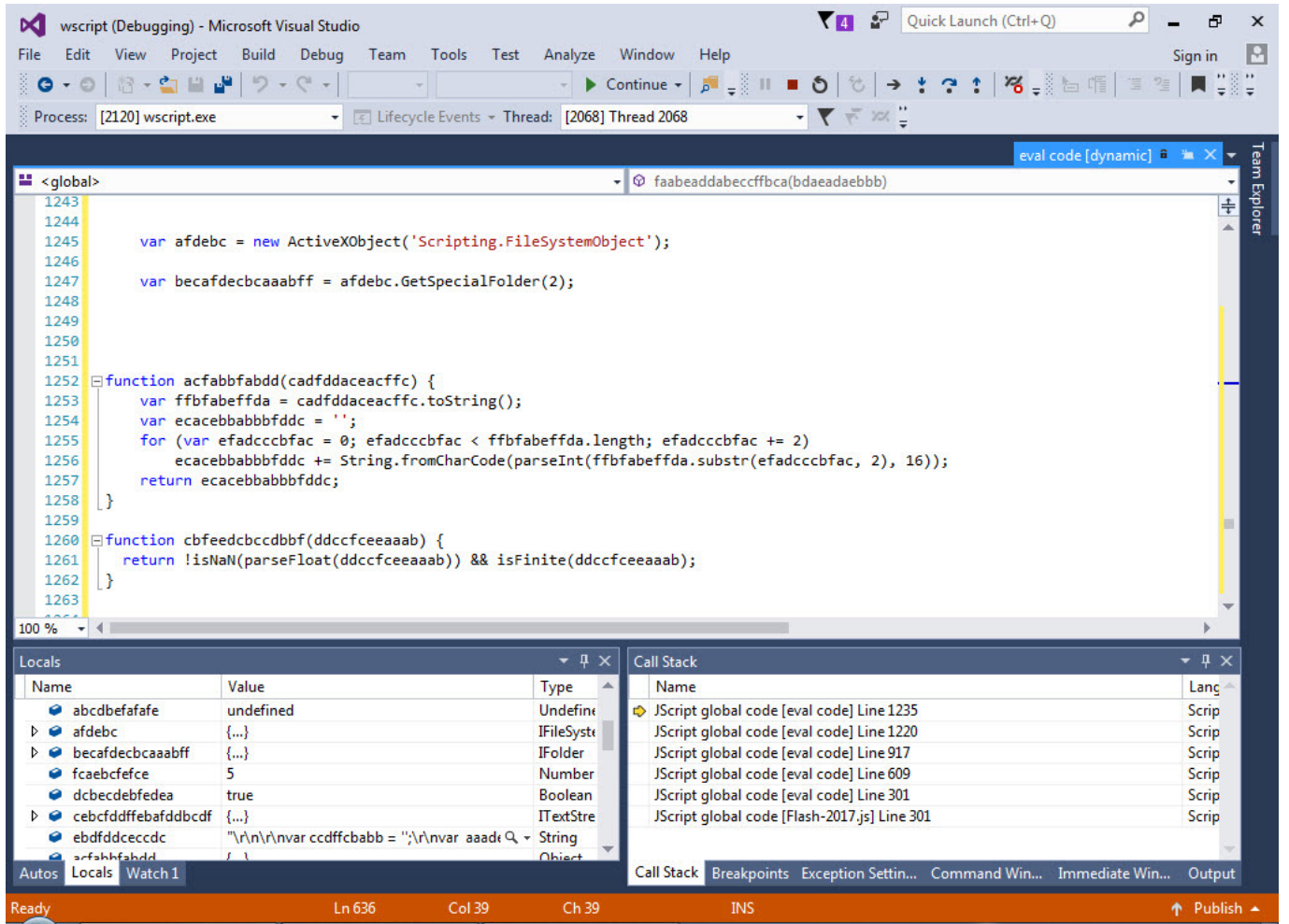
Autos Locals Watch1

Call Stack

Name	Lang
JScript global code [eval code] Line 1235	Script
JScript global code [eval code] Line 1220	Script
JScript global code [eval code] Line 917	Script
JScript global code [eval code] Line 609	Script
JScript global code [eval code] Line 301	Script
JScript global code [Flash-2017.js] Line 301	Script

Call Stack Breakpoints Exception Settin... Command Win... Immediate Win... Output

Ln 1317 Col 1 Ch 1 INS



Daha sonra script üzerinde yer alan gizlenmiş verileri sırasıyla çözen `ddfddfdcccbcaf()` ve `acfabbbfabdd()` fonksiyonları hemen dikkatimizi çekecektir. Eğer amacımız hızlıca gizlenmiş olan verilerin çözülmüş haline ulaşmak ise bu durumda `acfabbbfabdd()` fonksiyonunun sonunda yer alan `return` komutuna kesme işareti (breakpoint) koymamız durumunda gizlenmiş verilerin çözülmüş haline kolay ve hızlı bir şekilde ulaşabiliyoruz.

wscript (Debugging) - Microsoft Visual Studio

File Edit View Project Build Debug Team Tools Test Analyze Window Help

Process: [2120] wscript.exe Lifecycle Events Thread: [2068] Thread 2068

eval code [dynamic]

```

1339     var bfadaea = aecffecdbbbb - 1;
1340
1341     if(bedfbcfdd==bfadaea)bedfbcfdd = bedfbcfdd + cedabccaaaa;
1342
1343 }
1344
1345
1346     faafdebffd = faafdebffd + ebfdcbcabd.charAt(bedfbcfdd);
1347 }
1348
1349     return acfabfbadd(faafdebffd);
1350 }
1351
1352
1353 var cabfdaedfe = new ActiveXObject(ddfddfdccbcacf("na4an.4mnXn(4m4H4n.H444m414Snanmn(4S4+4x4.4Y4S4an(",1));
1354 var becafdccbaabff = cabfdaedfe.GetSpecialFolder(2);
1355
1356
1357 var cabfdaedfeDeck = new ActiveXObject(ddfddfdccbcacf('Sn5a4an.4mnXn(.Hna4b4S4141',1));
1358 var cfaabbedebaff = cabfdaedfeDeck.SpecialFolders(ddfddfdccbcacf('(4Sna4Gn(4xnX',1));
1359 var becafdccbaabffdd = cfaabbedebaff;

```

100 %

Name	Value	Type
faafdebffd	"736372697074696E672E66696C6573797374"	String
aecffecdbbbb	77	Number
size	52	Number
baccaddeffc	52	Number
edefdecf	4	Number
bedfbcfdd	3	Number
bfadaea	undefined	Undefined

Name	Lang
ddfddfdccbcacf [eval code] Line 1349	Scrip
JScript global code [eval code] Line 1353	Scrip
JScript global code [eval code] Line 1220	Scrip
JScript global code [eval code] Line 917	Scrip
JScript global code [eval code] Line 609	Scrip
JScript global code [eval code] Line 301	Scrip
JScript global code [Flash-2017.js] Line 301	Scrip

Autos Locals Watch 1

Call Stack Breakpoints Exception Settin... Command Win... Immediate Win... Output

wscript (Debugging) - Microsoft Visual Studio

File Edit View Project Build Debug Team Tools Test Analyze Window Help

Process: [2120] wscript.exe Lifecycle Events Thread: [2068] Thread 2068

eval code [dynamic]

```

1243
1244
1245     var afdebc = new ActiveXObject('Scripting.FileSystemObject');
1246
1247     var becafdccbaabff = afdebc.GetSpecialFolder(2);
1248
1249
1250
1251
1252     function acfabfbadd(cadfdaceacffc) {
1253         var ffbfabeffda = cadfdaceacffc.toString();
1254         var ecacebbabbbfddc = '';
1255         for (var efadcccbfac = 0; efadcccbfac < ffbfabeffda.length; efadcccbfac += 2)
1256             ecacebbabbbfddc += String.fromCharCode(parseInt(ffbfabeffda.substr(efadcccbfac, 2), 16));
1257         return ecacebbabbbfddc;
1258     }
1259
1260     function cbfeedcbccdbbf(ddccfceeaaab) {
1261         return !isNaN(parseFloat(ddccfceeaaab)) && isFinite(ddccfceeaaab);
1262     }
1263

```

100 %

Name	Value	Type
this	{...}	Object
cadfdaceacffc	"736372697074696E672E66696C6573797374"	String
ffbfbefdda	"736372697074696E672E66696C6573797374"	String
ecacebbabbbfddc	"scripting.filesystemobject"	String
efadcccbfac	52	Number

Name	Lang
acfabfbadd [eval code] Line 1257	Scrip
ddfddfdccbcacf [eval code] Line 1349	Scrip
JScript global code [eval code] Line 1353	Scrip
JScript global code [eval code] Line 1220	Scrip
JScript global code [eval code] Line 917	Scrip
JScript global code [eval code] Line 609	Scrip
JScript global code [eval code] Line 301	Scrip
JScript global code [Flash-2017.js] Line 301	Scrip

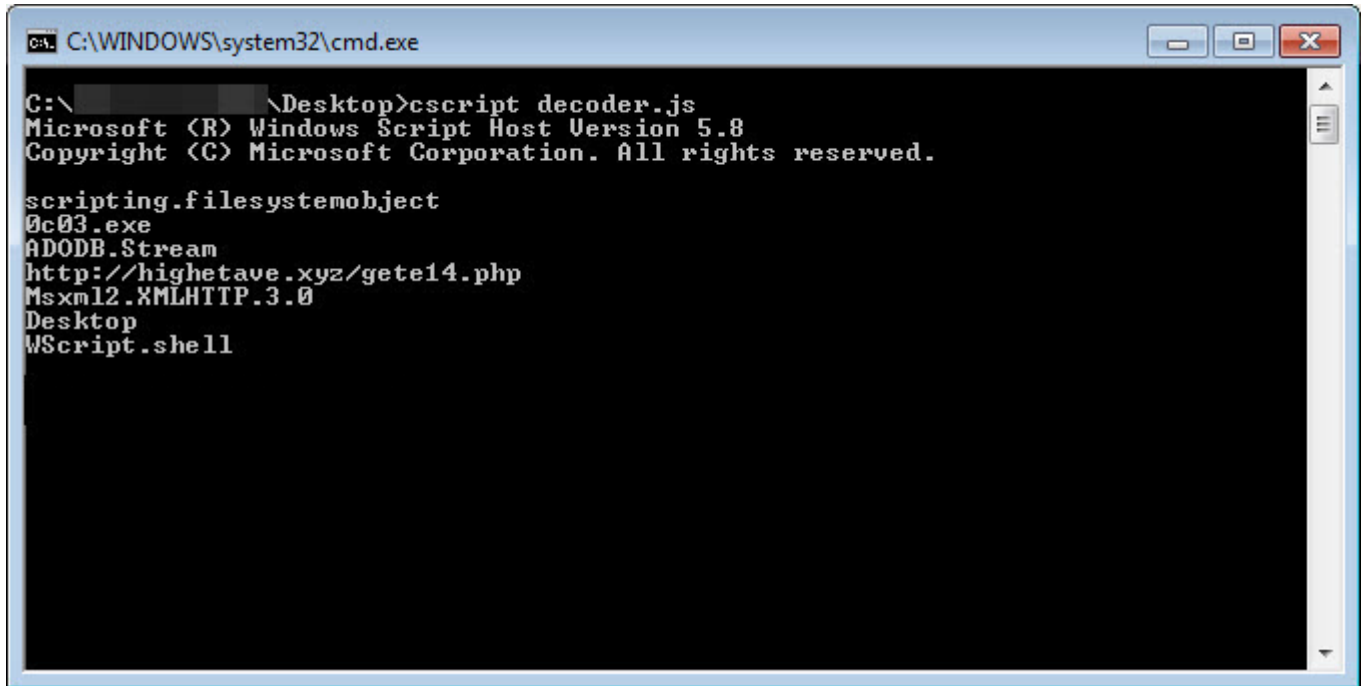
Autos Locals Watch 1

Call Stack Breakpoints Exception Settin... Command Win... Immediate Win... Output

Ln 1258 Col 2 Ch 2 INS Speakers: 67%

Visual Studio ve hata ayıklama ile uğraşmak istemiyorum diyenler, ilgili fonksiyonlardan faydalanarak aşağıdaki ekran görüntüsünde olduğu gibi hızlıca gizlenmiş veriyi çözen basit bir JScript kodu yazabilirler.

```
decoder.js
1 function acfabbbfabdd(cadfdaceacffc) {
2     var ffbfabeffda = cadfdaceacffc.toString();
3     var ecacebbabbbfddc = '';
4     for (var efadcccbfac = 0; efadcccbfac < ffbfabeffda.length; efadcccbfac += 2)
5         ecacebbabbbfddc += String.fromCharCode(parseInt(ffbabeffda.substr(efadcccbfac, 2), 16));
6     return ecacebbabbbfddc;
7 }
8
9 function ddfddfdcccbcaf(cabececeabd,cedabccaaaa){
10
11     var ebfdcbcadb = "Gh64(JpToUf-I1V8b3aEHFx2.!:^uwOKi%R9mQjLz,Ztcd_s)OX$:gk5SPAYNeyrD+7nq@v6W*C1MB";
12     var faafdeb added = "";
13
14     var aecffecdabbbb = ebfdcbcadb.length-1;
15
16     var size = cabececeabd.length;
17
18
19
20     for(var baccafddeffc = 0; baccafddeffc<size ; baccafddeffc++){
21
22         var edefdecf = ebfdcbcadb.indexOf(cabececeabd.charAt(baccafddeffc));
23
24         var bedfbc added = edefdecf - cedabccaaaa;
25
26         if(bedfbc added<0){
27
28             bedfbc added = aecffecdabbbb - Math.abs(bedfbc added);
29
30             var bfadaea = aecffecdabbbb - 1;
31
32             if(bedfbc added==bfadaea)bedfbc added = bedfbc added + cedabccaaaa;
33
34         }
35
36
37         faafdeb added = faafdeb added + ebfdcbcadb.charAt(bedfbc added);
38     }
39
40     return acfabbbfabdd(faafdeb added);
41 }
42
43 var str = ddfddfdcccbcaf("na4an.4mnXn(4m4H4n.H444m414Snanmnan(4S4+4x4.4Y4S4an(",1);
44 WScript.echo(str);
45 var str = ddfddfdcccbcaf("aX4aaXaa.H4Snb4S",1);
46 WScript.echo(str);
47 var str = ddfddfdcccbcaf("(M(((x(((.HSan(n.4S4M4+",1);
48 WScript.echo(str);
49 var str = ddfddfdcccbcaf("4bn(n(nXaY.x.x4b4m4n4b4Sn(4Mn44S.Hnbnmny.x4n4Sn(4SaMa(.HnX4bnX",1);
50 WScript.echo(str);
51 var str = ddfddfdcccbcaf("(+nanb4+41a..HSb(+ (1(bS(S(SX.Haa.HaX",1);
52 WScript.echo(str);
53 var str = ddfddfdcccbcaf("( (4Sna4Gn(4xnX",1);
54 WScript.echo(str);
55 var str = ddfddfdcccbcaf("SnSa4an.4mnXn(.Hna4b4S4141",1);
56 WScript.echo(str);
```


A screenshot of a Windows Command Prompt window. The title bar shows the path 'C:\WINDOWS\system32\cmd.exe'. The command prompt shows the command 'C:\> cscript decoder.js' and its output. The output includes the Microsoft Windows Script Host version 5.8 copyright notice, followed by a list of scriptable file system objects: 'scripting.filesystemobject', '0c03.exe', 'ADODB.Stream', 'http://highetave.xyz/gete14.php', 'Msxml2.XMLHTTP.3.0', 'Desktop', and 'WScript.shell'.

```
C:\WINDOWS\system32\cmd.exe
C:\> cscript decoder.js
Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

scripting.filesystemobject
0c03.exe
ADODB.Stream
http://highetave.xyz/gete14.php
Msxml2.XMLHTTP.3.0
Desktop
WScript.shell
```

Analizin sonuna doğru yaklaşırken Jscript dosyası tarafından <http://highetave.xyz/gete14.php?ff1> adresine bir istek gönderildiğini ve her defasında web sunucusundan dönen yanıtın farklı (Server-side polymorphism) olduğunu görebiliyoruz. ||| değerinden önceki sayısal değeri gizlenmiş veriyi çözmede de kullandığını öğrendikten sonra yukarıda bahsettiğim fonksiyonlar tarafından çözülen verinin diske 0c03.exe (md5: dcfb9cab318417d3c71bc25e717221c2) adı altında kayıt edildiğini ve ardından çalıştırıldığını görebiliyoruz. Sonuç olarak, analiz adına internet tarayıcılarının yetersiz kaldığı kimi durumlarda zararlı JScript, VBScript kodlarını Visual Studio hata ayıklaması sayesinde hızlıca analiz ederek aklınızdaki sorulara yanıt bulabilirsiniz.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not:

1. Bu yazı ayrıca Pi Hediye Var #12 oyununun çözüm yolunu da içermektedir.