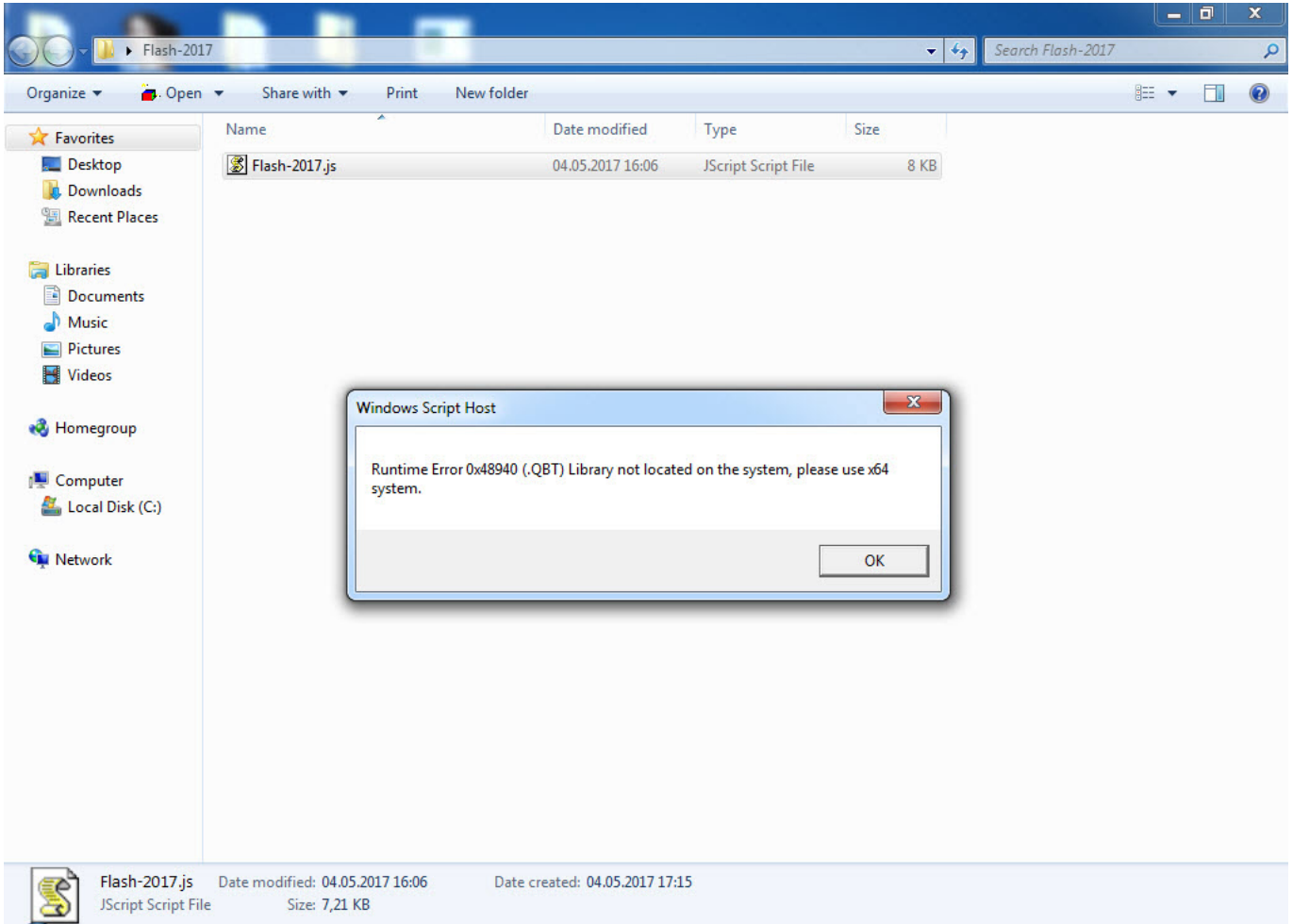


(W/C) script Hata Ayıklaması

written by Mert SARICA | 1 January 2018

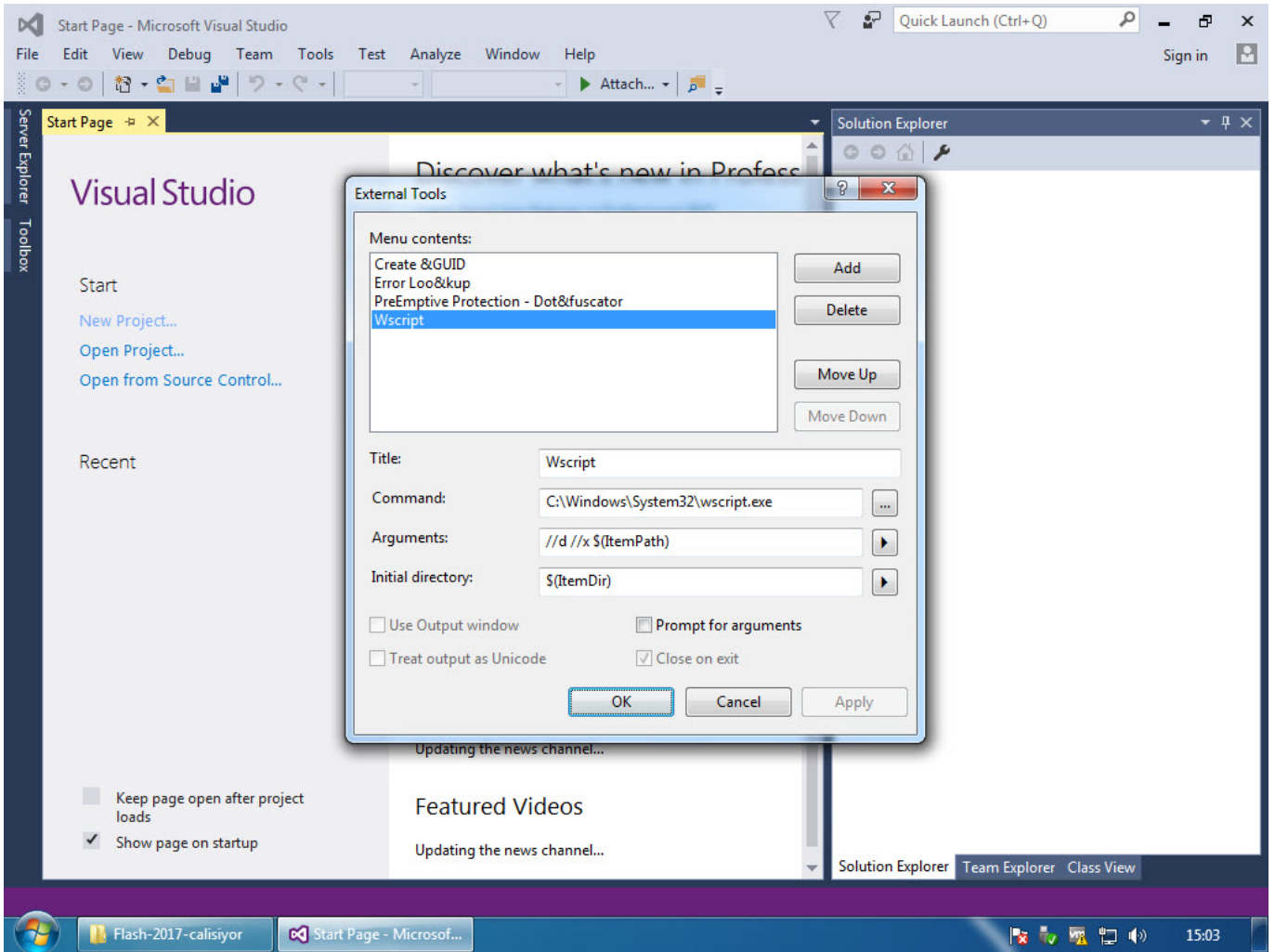
Okuyanlarınızın Man In The Proxy blog yazıma konu olan bir internet bankacılığı zararlı yazılımını hedef sisteme indirmek ve çalıştırmak amacıyla zararlı bir JScript dosyası (Flash-2017.js) kullanıldığını anımsayacaklardır. O yazıda okunaklı olmayan (encoded) bu JScript dosyasının Zararlı JavaScript 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.



```
Flash-2017.js
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 becafdcebcbaabff = afdebc.GetSpecialFolder(2);
16
17
18 /*
19
20 function acfabbbfabdd(cadfdaceacffc) {
21     var ffbfabeffda = cadfdaceacffc.toString();
22     var ecacebbabbbfddc = '';
23     for (var efadcccbfac = 0; efadcccbfac < ffbfabeffda.length; efadcccbfac += 2)
24         ecacebbabbbfddc += String.fromCharCode(parseInt(fffbfabeffda.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(eceedbbdaefeeceedbbdaefafe,bfadaea) {
35
36
37     for(i=bfadaea;i>0;i--){
38
39         eceedbbdaefeeceedbbdaefafe = eceedbbdaefeeceedbbdaefafe - 1;
40
41         if(eceedbbdaefeeceedbbdaefafe<0)eceedbbdaefeeceedbbdaefafe = 9;
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 teknolojisidir. 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.



```
Flash-2017.js* - Microsoft Visual Studio
File Edit View Project Debug Team Tools Test Analyze Window Help
Flash-2017.js* x
<global>
1
2
3 var ccdffcbabb = '';
4 var aaadeecfdeccae = [];
5 var abcdbefafafe;
6
7
8
9
10
11
12
13 var afdebc = new Activ
14
15 var becafedecbaaabff =
16
17
18 /*
19
20 function acfabbbabdd(cadfdaceacffc) {
21     var ffbfabeffda = cadfdaceacffc.toString();
22     var ecacebbabbbfddc = '';
23     for (var efadccbfac = 0; efadccbfac < ffbfabeffda.length; efadccbfac += 2)
24         ecacebbabbbfddc += String.fromCharCode(parseInt(fffbfabeffda.substr(efadccbfac, 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(eceedbbdaefeeceeedbbdaefefe,bfadaea){
35
```

This is not a valid location for a breakpoint. Ln 12 Col 5 Ch 2 INS Publish

Yazıma konu olan Flash-2017.js isimli JScript dosyasını adım adım hata ayıklama ile analiz etmeye başladığımızda, kodun yorum satırlarınının (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

Flash-2017.js [dynamic]

```

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

```

Name	Value	Type
this	{...}	Object
WScript	{...}	Object
WSH	{...}	Object
faabeaddabecffba	{...}	Object
ccdfccbabb	undefined	Undefin
aaadeecfdeccae	undefined	Undefin
abcdbefafafe	undefined	Undefin
afdebc	undefined	Undefin

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

```

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

```

Name	Value	Type
abcdbefafafe	undefined	Undefin
afdebc	{...}	IFileSyste
becafdecbaabff	{...}	IFolder
fcaebcfce	5	Number
dcbecdefedea	true	Boolean
cebcdffebafddbcdf	{...}	ITextStre
ebfddecccddc	"\\.\nvar ccdfccbabb = \";\\.\nvar aaad	String
acfabbfabdd		Object

Name	Lang
JScript global code [eval code] Line 1235	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 1317 Col 1 Ch 1 INS

The screenshot shows the Microsoft Visual Studio interface during a debugging session. The main editor window displays JavaScript code with a breakpoint at line 1257. The code includes variables for file system objects and a function that processes a string. The Locals window shows the current state of variables, and the Call Stack window shows the execution path.

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

Name	Value	Type
abdcbefafafe	undefined	Undefined
afdebc	{...}	IFileSystemObject
becafdecbaabff	{...}	IFolder
fcaebcfefce	5	Number
dcbecdefedea	true	Boolean
cebcdffefebafddbcdf	{...}	ITextStream
ebfddeccecdc	"\\n\\n\\nvar ccdfcbabb = "\\n\\nvar aaad..."	String
acfabbbabdd	function	Function

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

Daha sonra script üzerinde yer alan gizlenmiş verileri sırasıyla çözen `ddfddfdcccbaaf()` 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 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

```

1339     var bfadaea = aeccfedabbbb - 1;
1340
1341     if(bedfbcfdd==bfadaea)bedfbcfdd = bedfbcfdd + cedabccaaaa;
1342
1343 }
1344
1345
1346     faafdebfgdd = faafdebfgdd + ebdfbcadb.charAt(bedfbcfdd);
1347 }
1348
1349     return acfabbbabdd(faafdebfgdd);
1350 }
1351
1352
1353 var cabfdaedfe = new ActiveXObject(ddfddfcccbcac('na4an.4mnXn(4m4H4n.H444m414Snanmnan(4S4+4x4.4Y4S4an(",1));
1354 var becafdccbaabff = cabfdaedfe.GetSpecialFolder(2);
1355
1356
1357 var cabfdaedfeDeck = new ActiveXObject(ddfddfcccbcac('Sn5a4an.4mnXn(.Hna4b4S4141',1));
1358 var cfaabbedeaeaff = cabfdaedfeDeck.SpecialFolders(ddfddfcccbcac('(4Sna4Gn(4xnX',1));
1359 var becafdccbaabffdd = cfaabbedeaeaff;

```

Locals

Name	Value	Type
faafdebfgdd	"736372697074696E672E66696C6573797374"	String
aeccfedabbbb	77	Number
size	52	Number
baccafdeffc	52	Number
edefdecf	4	Number
bedfbcfdd	3	Number
bfadaea	undefined	Undefined

Call Stack

Name	Lang
ddfddfcccbcac [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

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

```

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

```

Locals

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

Call Stack

Name	Lang
acfabbbabdd [eval code] Line 1257	Script
ddfddfcccbcac [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

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.

```
decoderjs
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(ffbfabeffda.substr(efadcccbfac, 2), 16));
6   return ecacebbabbbfddc;
7 }
8
9 function ddfddfdcccbcacf(cabececeabd,cedabccaaaa){
10
11   var ebfdcbcadb = "Gh64(JpToUf-IIV8b3aEHFx2.!:^uwOKi%R9mQjLz,Ztcd_s)OX$:gk5SPAYNeyrD+7nq@v6W*C1MB";
12   var faafdebfd = "";
13
14   var aecffecdabbbb = ebfdcbcadb.length-1;
15
16   var size = cabececeabd.length;
17
18
19
20   for(var baccafdeeffc = 0; baccafdeeffc<size ; baccafdeeffc++){
21
22     var edefdecf = ebfdcbcadb.indexOf(cabececeabd.charAt(baccafdeeffc));
23
24     var bedfbcfdd = edefdecf - cedabccaaaa;
25
26     if(bedfbcfdd<0){
27
28       bedfbcfdd = aecffecdabbbb - Math.abs(bedfbcfdd);
29
30       var bfadaea = aecffecdabbbb - 1;
31
32       if(bedfbcfdd==bfadaea)bedfbcfdd = bedfbcfdd + cedabccaaaa;
33
34     }
35
36
37     faafdebfd = faafdebfd + ebfdcbcadb.charAt(bedfbcfdd);
38
39
40   }
41
42   return acfabbbfabdd(faafdebfd);
43
44   var str = ddfddfdcccbcacf("na4an.4mnXn(4m4H4n.H444m4l4Snanmnan(4S4+4x4.4Y4S4an",1);
45   WScript.echo(str);
46   var str = ddfddfdcccbcacf("aX4aaXaa.H4Snb4S",1);
47   WScript.echo(str);
48   var str = ddfddfdcccbcacf("M(((x(((..HSan(n.4S4M4+",1);
49   WScript.echo(str);
50   var str = ddfddfdcccbcacf("4bn(n(nXaY.x.x4b4m4n4b4Sn(4Mn44S.Hnbnmny.x4n4Sn(4SaMa(.HnX4bnX",1);
51   WScript.echo(str);
52   var str = ddfddfdcccbcacf("(+nanb4+41a..HSb(+1(bS(S(SX.Haa.HaX",1);
53   WScript.echo(str);
54   var str = ddfddfdcccbcacf("(4Sna4Gn(4xnX",1);
55   WScript.echo(str);
56   var str = ddfddfdcccbcacf("SnSa4an.4mnXn(.Hna4b4S4141",1);
57   WScript.echo(str);
58 }
```



```
C:\WINDOWS\system32\cmd.exe
C:\[redacted]\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://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 çözmeye 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 Hediyem Var #12 oyununun çözüm yolunu da içermektedir.