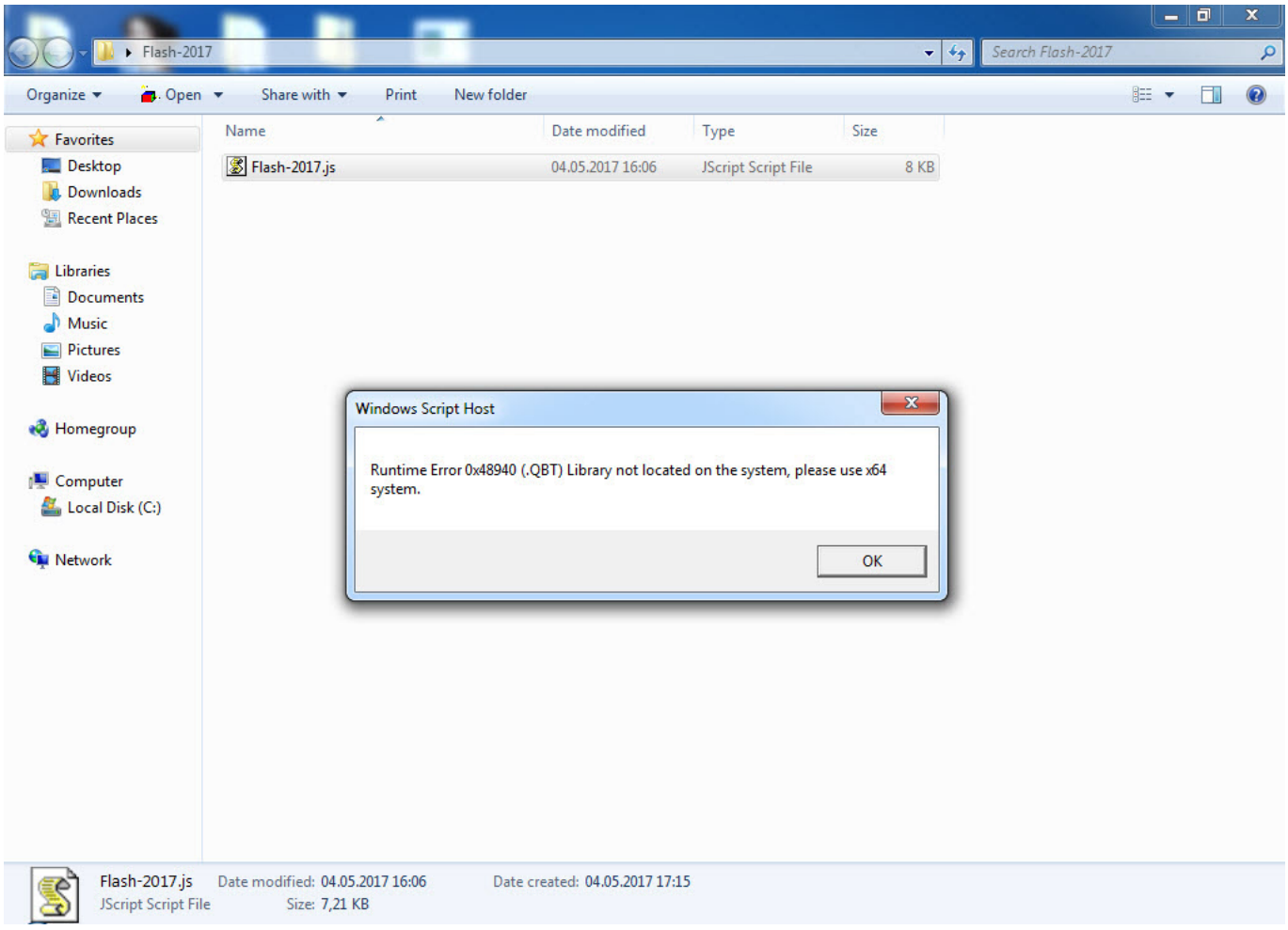
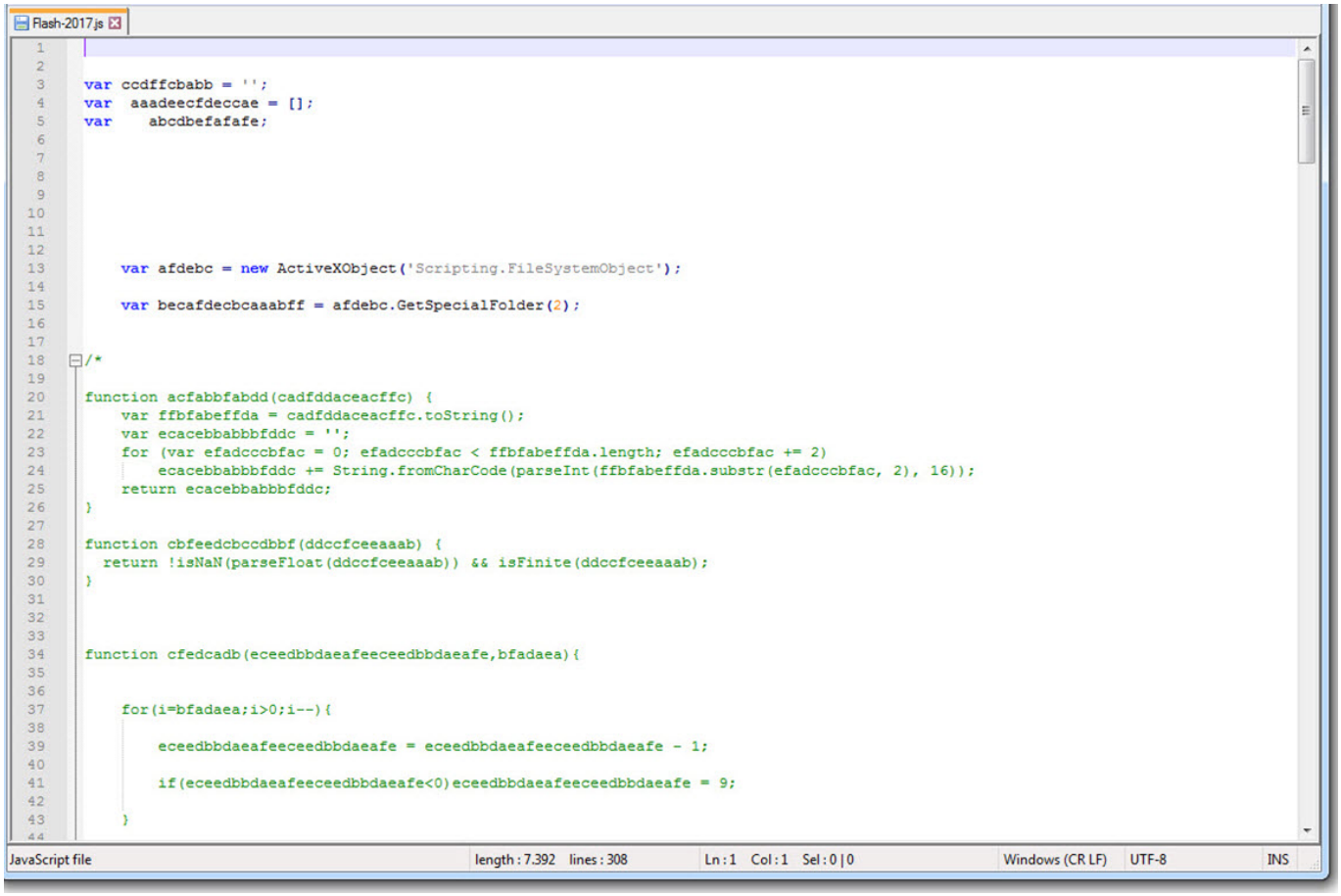
(W/C)script Hata Ayıklaması

written by Mert SARICA | 1 January 2018

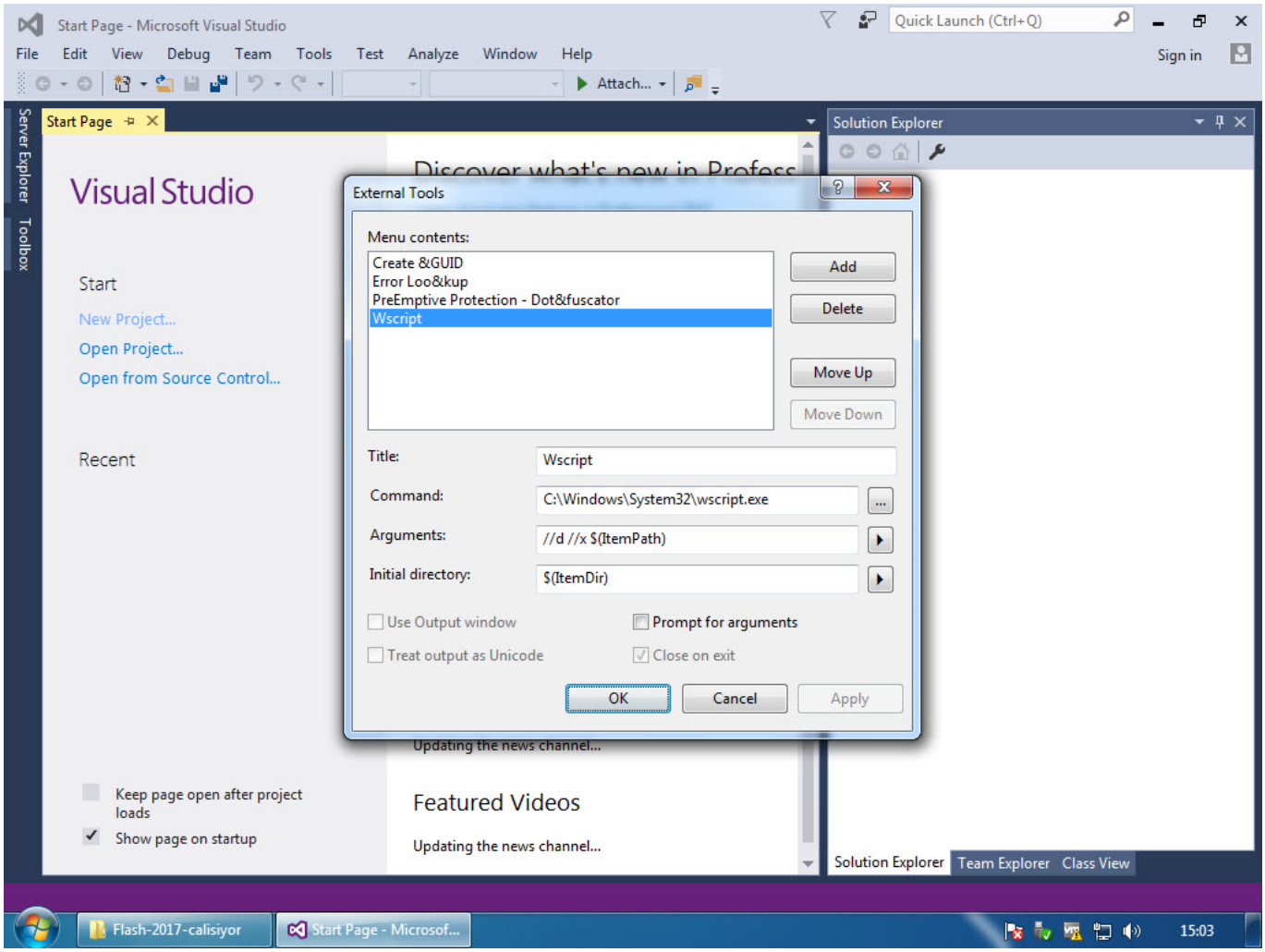
Okuyanlarınız Man In The Proxy blog yazıma konu olan bir internet bankacılığı zararlı yazılımını hedef sisteme indirmek ve çalıştırmak amacıyla zararlı bir JScript dosyası (Flash-2017.js) kullanıldığını anımsayacaklardır. O yazıda okunaklı olmayan (encoded) bu JScript dosyasının Zararlı JavaScript Analizi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

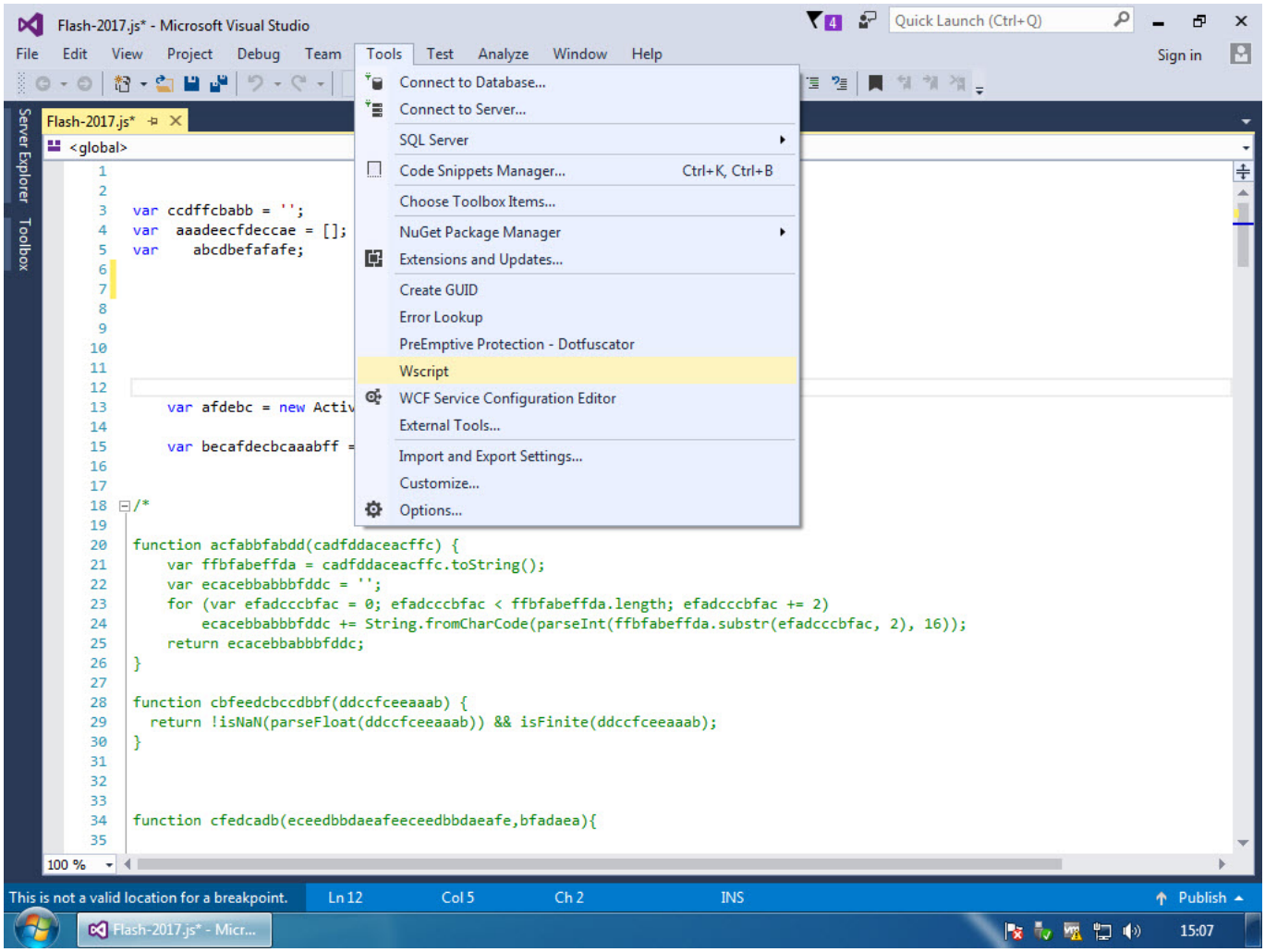




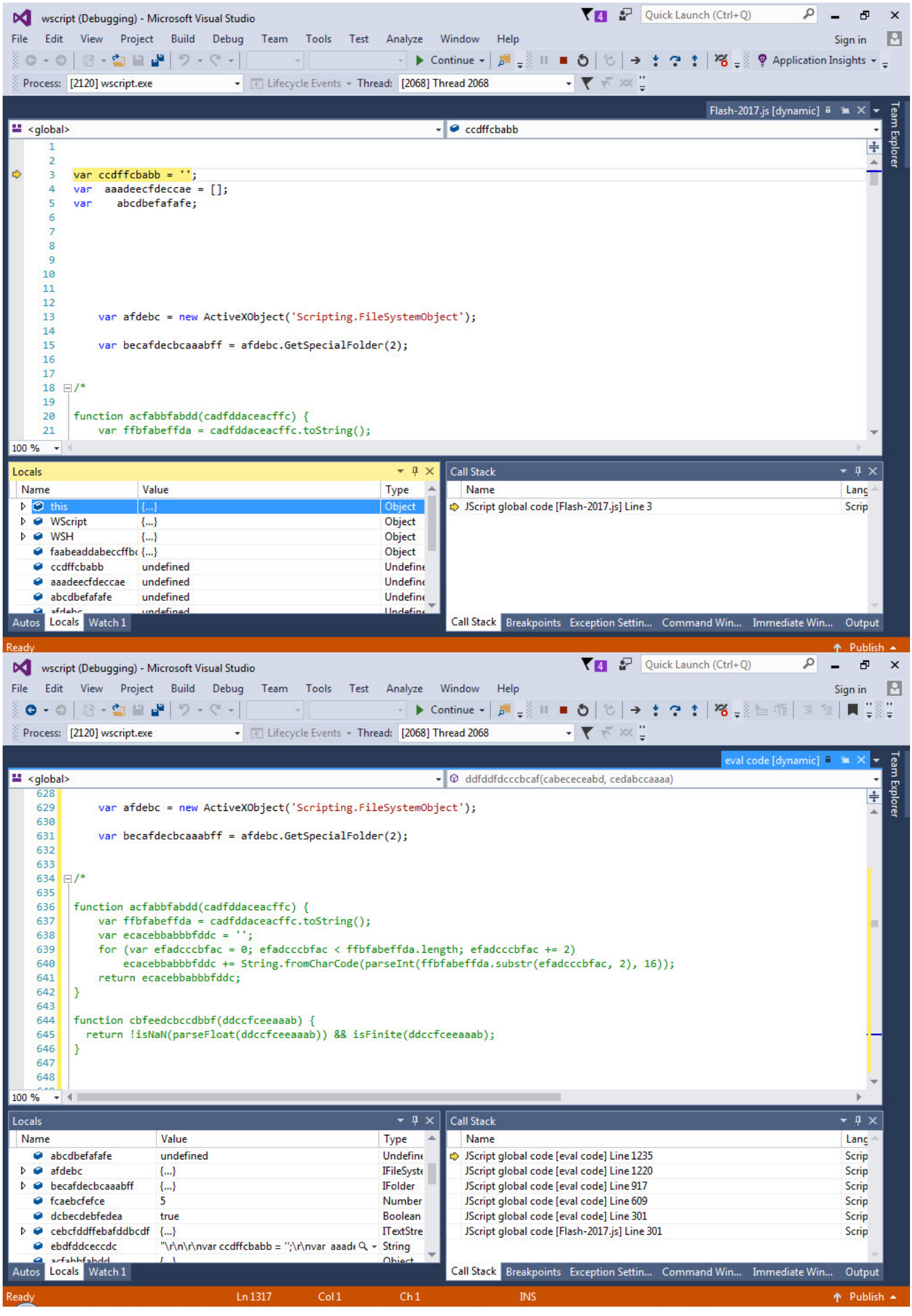
Wikipedia‘ya göre Microsoft Windows Script Host (WSH) (eski adıyla Windows Scripting Host), Microsoft Windows işletim sistemine özellik açısından BATCH dosyalarına kıyasla çok daha fazlasını vadeden bir betik otomasyon teknolojisidir. Birden fazla betik (JScript, VBSscript) dosyasını desteklemesi en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

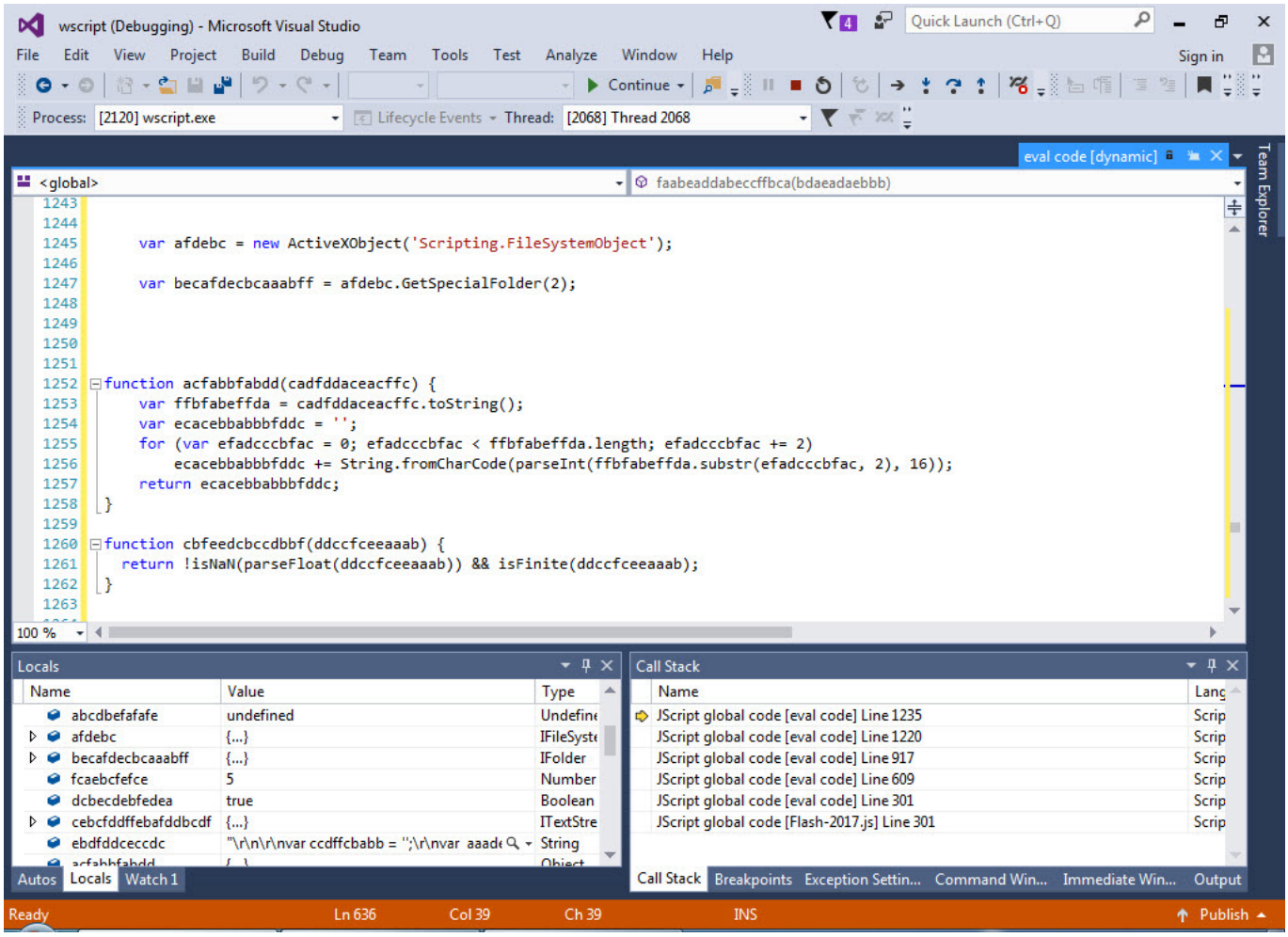
Bu gibi durumlarda JScript dosyasını hızlıca analiz edebilmek için ilk olarak Visual Studio’da, Tools -> External Tools menüsü altında Microsoft tarafından belirtilen hata ayıklama parametrelerini tanımlamalısınız. Ardından analiz etmek istediğiniz JScript dosyasını Visual Studio’da açtıktan sonra Tools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


Start Page - Microsoft Visual Studio
File Edit View Debug Team Tools Test Analyze Window Help
Quick Launch (Ctrl+Q)
Sign in
Attach...
Server Explorer
Toolbox
Start Page
Visual Studio
Start
New Project...
Open Project...
Open from Source Control...
Recent
Keep page open after project loads
Show page on startup
Updating the news channel...
Featured Videos
Updating the news channel...
Solution Explorer
Solution Explorer Team Explorer Class View
External Tools
Menu contents:
Create &GUID
Error Loo&kup
PreEmptive Protection - Dot&fuscator
Wscript
Add
Delete
Move Up
Move Down
Title: Wscript
Command: C:\Windows\System32\wscript.exe
Arguments: //d //x $(ItemPath)
Initial directory: $(ItemDir)
Use Output window
Prompt for arguments
Treat output as Unicode
Close on exit
OK
Cancel
Apply
Flash-2017-calisiyor
Start Page - Microsof...
15:03

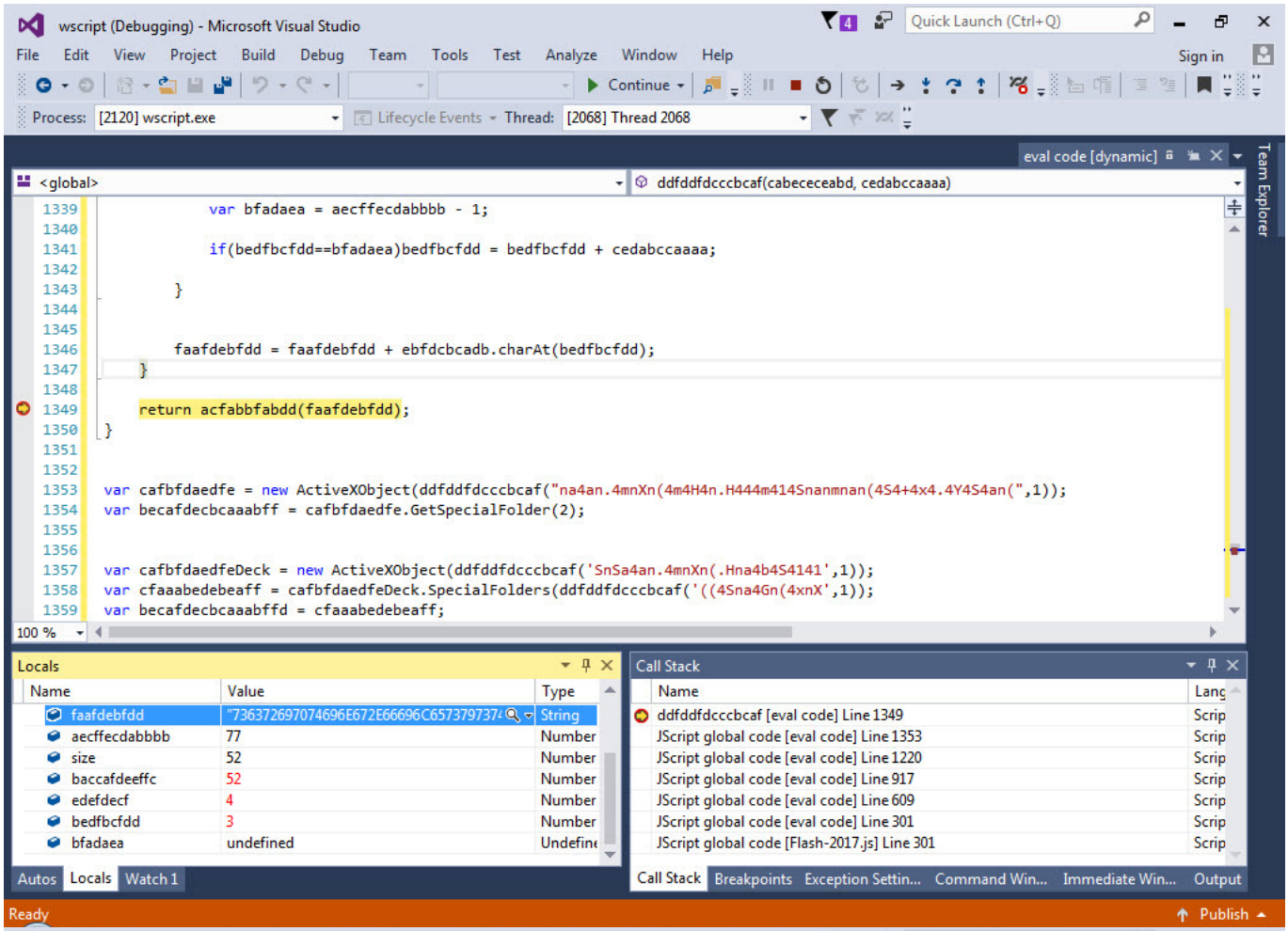


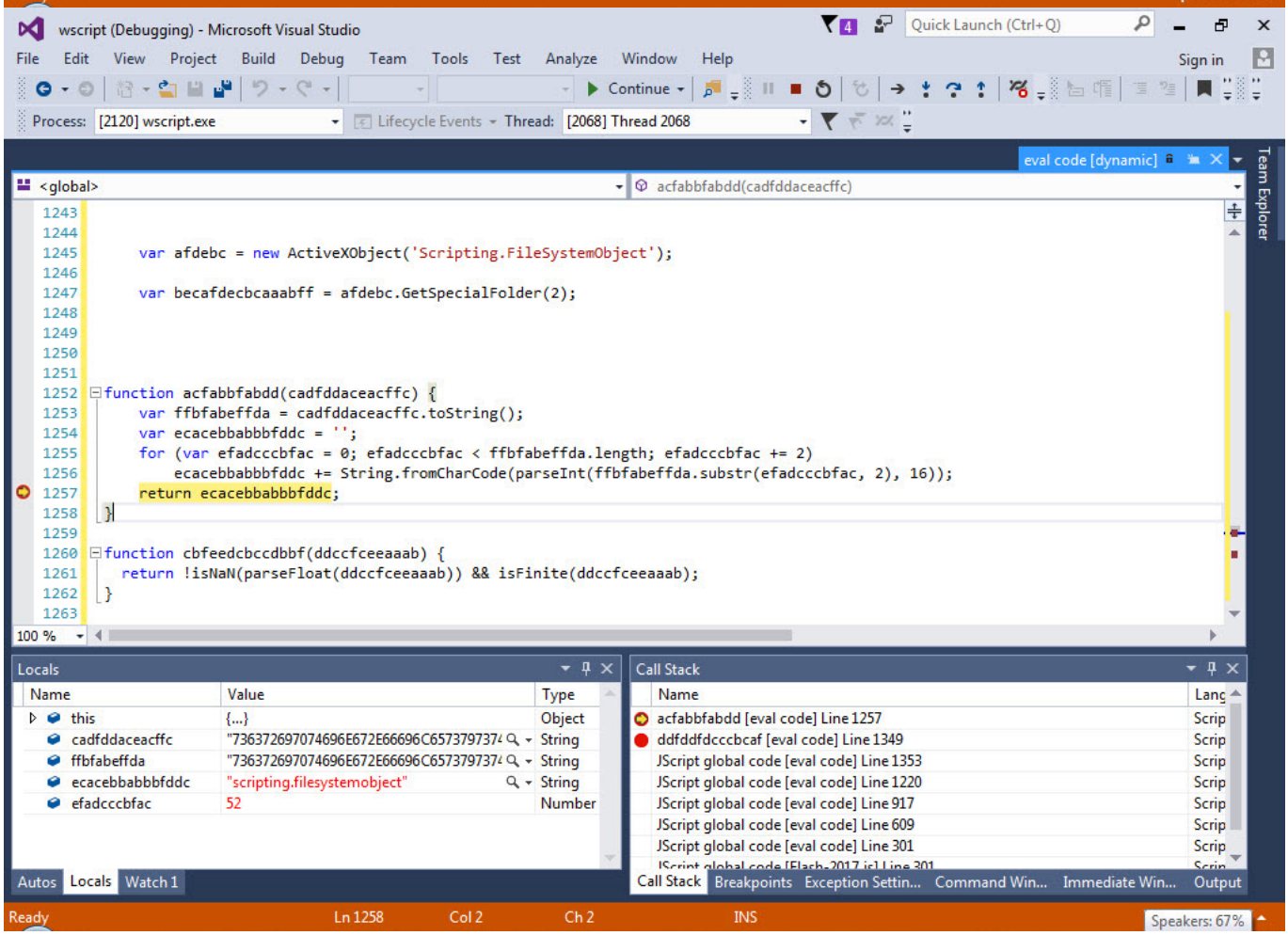
Yazıma konu olan Flash-2017.js isimli JScript dosyasını adım adım hata ayıklama ile analiz etmeye başladığımızda, kodun yorum satırlarının (comment) başındaki /* ve */ karakterleri sildiğini görebiliyoruz.


wscript (Debugging) - Microsoft Visual Studio
Quick Launch (Ctrl+Q)
File Edit View Project Build Debug Team Tools Test Analyze Window Help
Sign in
Continue
Application Insights
Process: [2120] wscript.exe
Lifecycle Events
Thread: [2068] Thread 2068
Flash-2017.js [dynamic]
Team Explorer
<global>
ccdffcbabb
var ccdffcbabb = '';
var aaadeecfdeccae = [];
var abcdbefafafe;
var afdebc = new ActiveXObject('Scripting.FileSystemObject');
var becafdecbcaaabff = afdebc.GetSpecialFolder(2);
/*
function acfabbfabdd(cadfddaceacffc) {
var ffbfabeffda = cadfddaceacffc.toString();
100 %
Locals
Name Value Type
this {...} Object
WScript {...} Object
WSH {...} Object
faabeaddabeccffbc {...} Object
ccdffcbabb undefined Undefine
aaadeecfdeccae undefined Undefine
abcdbefafafe undefined Undefine
Call Stack
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
Ready
Publish
wscript (Debugging) - Microsoft Visual Studio
Quick Launch (Ctrl+Q)
File Edit View Project Build Debug Team Tools Test Analyze Window Help
Sign in
Continue
Process: [2120] wscript.exe
Lifecycle Events
Thread: [2068] Thread 2068
eval code [dynamic]
Team Explorer
<global>
ddfddfdcccbcaf(cabececeabd, cedabccaaaa)
var afdebc = new ActiveXObject('Scripting.FileSystemObject');
var becafdecbcaaabff = afdebc.GetSpecialFolder(2);
/*
function acfabbfabdd(cadfddaceacffc) {
var ffbfabeffda = cadfddaceacffc.toString();
var ecacebbabbbfddc = '';
for (var efadcccbfac = 0; efadcccbfac < ffbfabeffda.length; efadcccbfac += 2)
ecacebbabbbfddc += String.fromCharCode(parseInt(ffbfabeffda.substr(efadcccbfac, 2), 16));
return ecacebbabbbfddc;
}
function cbfeedcbccdbbf(ddccfceeaaab) {
return !isNaN(parseFloat(ddccfceeaaab)) && isFinite(ddccfceeaaab);
}
100 %
Locals
Name Value Type
abcdbefafafe undefined Undefine
afdebc {...} IFileSyste
becafdecbcaaabff {...} IFolder
fcaebcfefce 5 Number
dcbecdebfedea true Boolean
cebcfddffebafddbcdf {...} ITextStre
ebdfddceccdc "\r\n\r\nvar ccdffcbabb = '';\r\nvar aaade String
Call Stack
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
Ready
Ln 1317
Col 1
Ch 1
INS
Publish

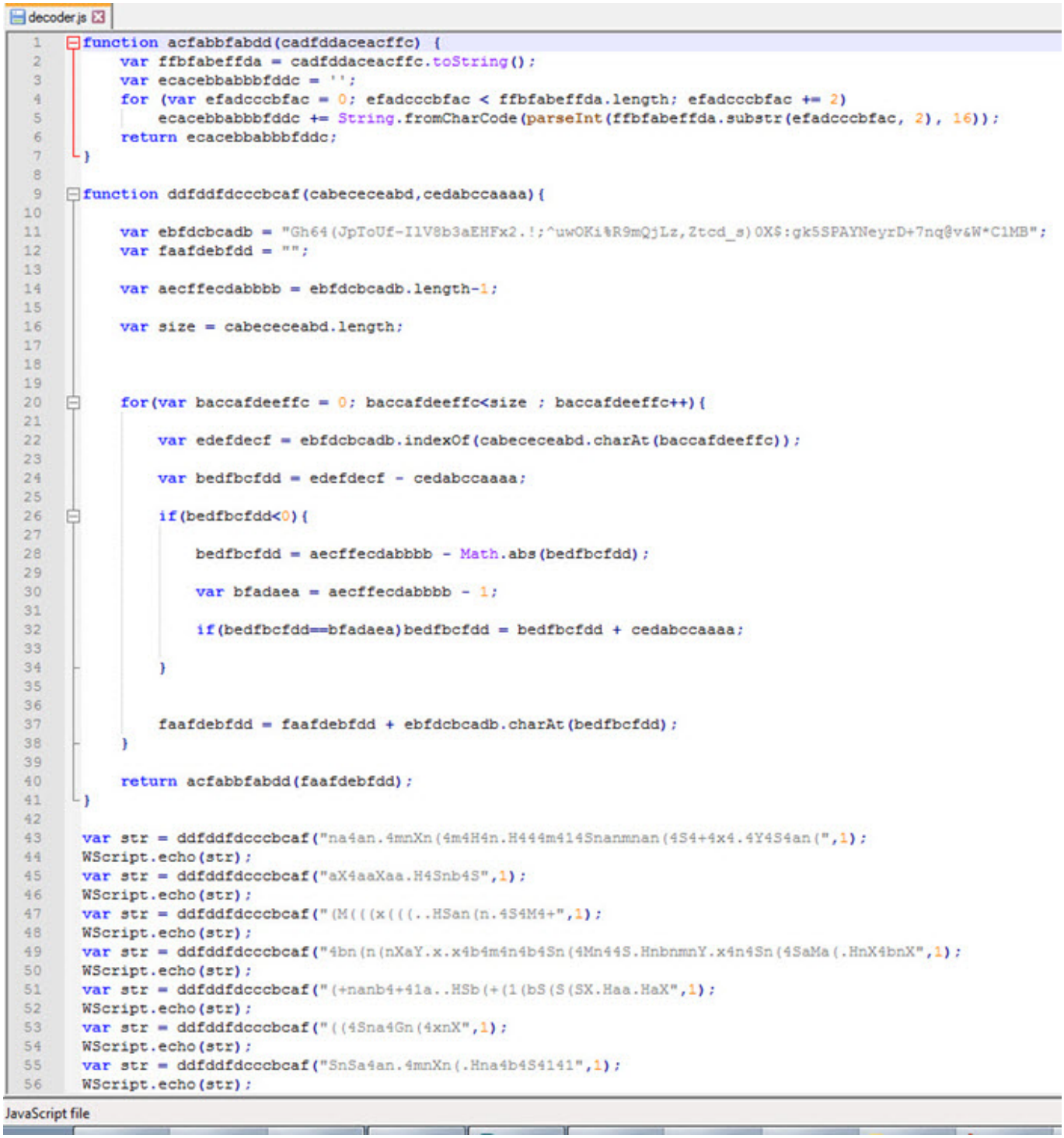


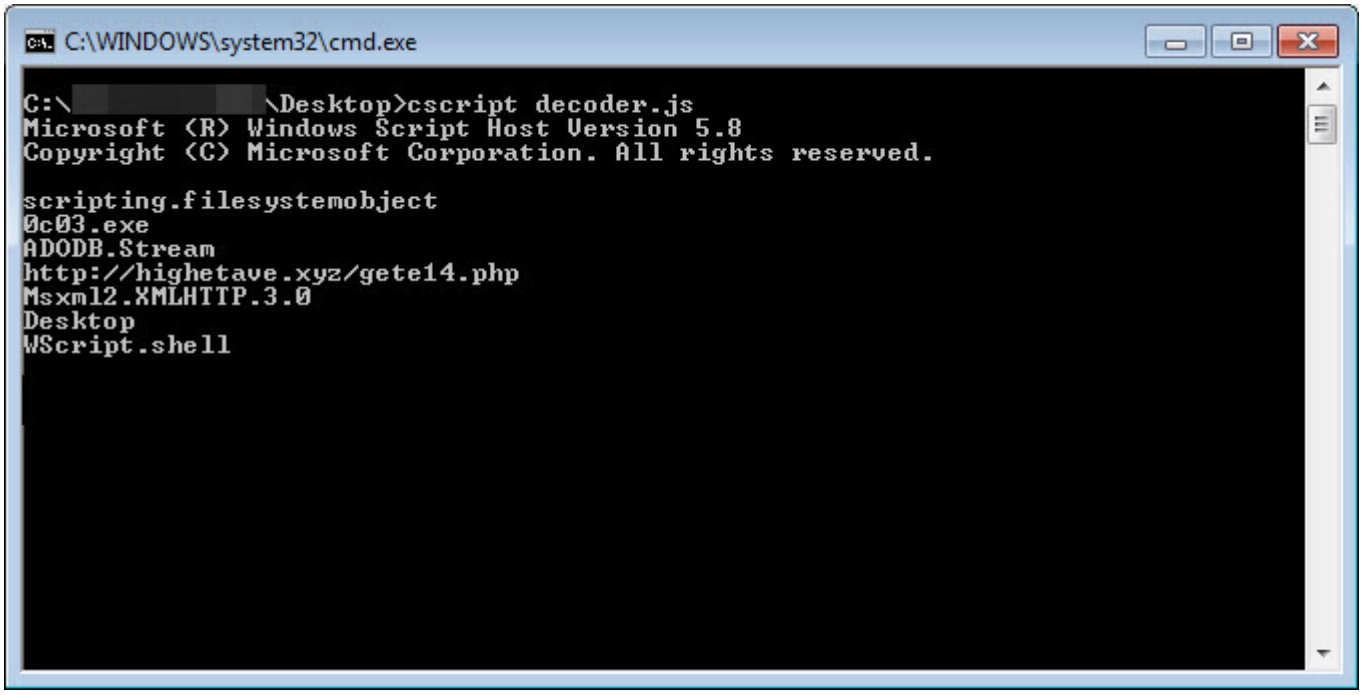
Daha sonra script üzerinde yer alan gizlenmiş verileri sırasıyla çözen ddfddfdcccbcaf() ve acfabbfabdd() fonksiyonları hemen dikkatimizi çekecektir. Eğer amacımız hızlıca gizlenmiş olan verilerin çözülmüş haline ulaşmak ise bu durumda acfabbfabdd() fonksiyonunun sonunda yer alan return komutuna kesme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


wscript (Debugging) - Microsoft Visual Studio
Quick Launch (Ctrl+Q)
File Edit View Project Build Debug Team Tools Test Analyze Window Help
Sign in
Continue
Process: [2120] wscript.exe
Lifecycle Events
Thread: [2068] Thread 2068
eval code [dynamic]
<global>
ddfdddfdcccbcaf(cabececeabd, cedabccaaaa)
1339 var bfadaea = aecffecdabbbb - 1;
1340
1341 if(bedfbcfdd==bfadaea)bedfbcfdd = bedfbcfdd + cedabccaaaa;
1342
1343 }
1344
1345
1346 faafdebfdd = faafdebfdd + ebfdcbcadb.charAt(bedfbcfdd);
1347 }
1348
1349 return acfabbfabdd(faafdebfdd);
1350 }
1351
1352
1353 var cafbfdaedfe = new ActiveXObject(ddfdddfdcccbcaf("na4an.4mnXn(4m4H4n.H444m414Snanmnan(4S4+4x4.4Y4S4an(",1));
1354 var becafdecbcaaabff = cafbfdaedfe.GetSpecialFolder(2);
1355
1356
1357 var cafbfdaedfeDeck = new ActiveXObject(ddfdddfdcccbcaf('SnSa4an.4mnXn(.Hna4b4S4141',1));
1358 var cfaaabedebeaff = cafbfdaedfeDeck.SpecialFolders(ddfdddfdcccbcaf('((4Sna4Gn(4xnX',1));
1359 var becafdecbcaaabffd = cfaaabedebeaff;
100 %
Locals
Name Value Type
faafdebfdd "736372697074696E672E66696C6573797374 String
aecffecdabbbb 77 Number
size 52 Number
baccafdeeffc 52 Number
edefdecf 4 Number
bedfbcfdd 3 Number
bfadaea undefined Undefine
Autos Locals Watch 1
Call Stack
Name Lang
ddfdddfdcccbcaf [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
Call Stack Breakpoints Exception Settin... Command Win... Immediate Win... Output
Ready
Publish
Team Explorer


wscript (Debugging) - Microsoft Visual Studio
Quick Launch (Ctrl+Q)
File Edit View Project Build Debug Team Tools Test Analyze Window Help
Sign in
Continue
Process: [2120] wscript.exe
Lifecycle Events
Thread: [2068] Thread 2068
eval code [dynamic]
<global>
acfabbfabdd(cadfddaceacffc)
1243
1244
1245 var afdebc = new ActiveXObject('Scripting.FileSystemObject');
1246
1247 var becafdecbcaaabff = afdebc.GetSpecialFolder(2);
1248
1249
1250
1251
1252 function acfabbfabdd(cadfddaceacffc) {
1253 var ffbfabeffda = cadfddaceacffc.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 %
Locals
Name Value Type
this {...} Object
cadfddaceacffc "736372697074696E672E66696C6573797374 String
ffbfabeffda "736372697074696E672E66696C6573797374 String
ecacebbabbbfddc "scripting.filesystemobject" String
efadcccbfac 52 Number
Autos Locals Watch 1
Call Stack
Name Lang
acfabbfabdd [eval code] Line 1257 Scrip
ddfdddfdcccbcaf [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
Call Stack Breakpoints Exception Settin... Command Win... Immediate Win... Output
Ready
Ln 1258 Col 2 Ch 2 INS
Speakers: 67%
Team Explorer

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.





Analizin sonuna doğru yaklaşırken Jscript dosyası tarafından http://highetave.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 Hediyem Var #12 oyununun çözüm yolunu da içermektedir.