Trojan Haftası

written by Mert SARICA | 7 November 2010

Müşterilerinden gelen ihbarlar nedeniyle bankalar geçtiğimiz haftaya hızlı başladılar. Özellikle Salı gününe MIB (Man in the mobile) saldırısı gerçekleştirebilen Zeus trojanı damgasını vurdu. Yaklaşık 1 ay önce Netsec'in 35. sayısında bu trojana değinmiş ve yakın zamanda bu yöntemi kullanan trojanlar ile karşılaşabileceğimizi belirtmiştim ki çok geçmeden Türkiye'deki bazı bankaları hedef alarak ortaya çıkıverdi.

Gelen ihbarların çoğu bankaların internet bankacılığı giriş sayfasında şüpheli bir pencerenin açıldığı, TCKN ve cep telefonu bilgilerinin istendiği yönünde oldu. Daha sonra gelen ihbarlar ise cep telefonuna bir sms gönderildiği ve mesajda bir adresin yer aldığı ve bu adresteki zararlı yazılımı kuran kişilerin internet bankacılığına girişte ve bankacılık işlemlerinde kullanmış oldukları SMS kodlarının çalındığı yönünde oldu. İlk başta işin içinde tek bir trojanın olduğunu düşünülsede çok geçmeden farklı kaynaklardan toplanan bilgiler bir araya getirilerek iki farklı trojanın olduğu ortaya çıktı.

Trojanlardan biri, kullanıcının, trojanın üzerinde tanımlı olan PTT (interaktif posta çeki sayfası), Paypal, bir hacking forumu ve 19 tane bankaya ait olan internet bankacılığı sayfalarından bir tanesine girmesi durumunda kullanıcı adı ve şifresini çalıyor, ekran görüntülerini diske kayıt ediyor ve eğer ziyaret edilen site bu 19 bankadan bir tanesinin internet bankacılığı sitesi ise ilave olarak yeni bir pencere açarak TCKN ve cep telefonu bilgilerini alıyor ve bir ftp sunucusuna gönderiyor diğeri ise, nam-ı diğer Zeus, internet bankacılığı kullanıcı adı ve şifresini çalmakla yetinmeyip kullanıcıdan cep telefonu numarası, cep telefonu marka ve model bilgilerinide isteyerek cep telefonuna zararlı bir yazılım, trojan göndererek cep telefonuna gelen SMS'leri çalıyordu.

TCKN ve cep telefonu bilgisi toplayan trojan, e-posta yolu ile yayılıyor ve bilgi güvenliğinin en zayıf halkası olan insanı istismar ediyordu.

From: HABERTÜRK [mailto:haber@haberturk.com]
Sent: Monday, November 01, 2010 7:15 PM
Subject: ' VARAN 2 ' DENİZ BAYKAL' A İKİNCİ ŞOK.. DENİZ BAYKALIN İKİNCİ SEX VİDEOSUNU YAYIMLIYORUZ

HABERTURK.COM TÜRKİYENİN
EN BÜYÜK İNTERNET GAZETESİ

DAHA ÖNCE 1. CİSİ YAYINLANAN DENİZ BAYKAL
VE NESRİN BAYTOK'UN SEKS GÖRÜNTÜLERİNİN
2.SİDE VARAN 2 ADIYLA HABER
MÜDÜRLÜĞÜMÜZE GÖNDERİLDİ.YAYIN YASAĞI
NEDENİ İLE HABERLERİMİZDE
YAYINLAYAMADIĞIMIZ GÖRÜNTÜLERİ İNTERNET
ÜZERİNDEN SİZLERE SUNUYORUZ.

video.haberturk.rar
340K Download

Rar dosyası açıldığında içinden video.haberturk.com adında bir dosya çıkıyordu. 2 Kasım tarihinde dosyayı VirusTotal sitesinde tarattığımda sadece 5 tane antivirüs (DrWeb, Sunbelt, Panda, Kaspersky, Prevx), 3 Kasım tarihinde tarattığımda ise 6 tane antivirüs (DrWeb, Sunbelt, Panda, Kaspersky, Prev, NOD32) bunu zararlı yazılım olarak tespit ediyordu. (Şu an itibariyle ise sadece 9 tane antivirüs (DrWeb, Sunbelt, Panda, Kaspersky, McAfee, McAfee-GW-Edition, Fortinet, AntiVir, NOD32) bu dosyayı tanıyor.)

TCKN ve cep telefonu bilgisi toplayan trojana ait dosyaları statik olarak analiz ettiğimde;

- Video.haberturk.com dosyasının Delphi programlama dili ile programlandığını,
- Son olarak 1 Kasım tarihinde değiştirildiğini,
- ftp.my3gb.com sunucusuna (ftp şifresi değiştiği ve my3gb yöneticileri tarafından hesap silindiği için sunucu adını ifşa ediyorum) bağlanma ihtimali olduğunu,
- Kayıt altına alınan ve sunucuya gönderilen dosyaların başkaları tarafından çalınmaması adına ftp kullanıcı adı, şifre, port ve bazı bilgileri şifreleyerek sakladığını söyleyebilirim.

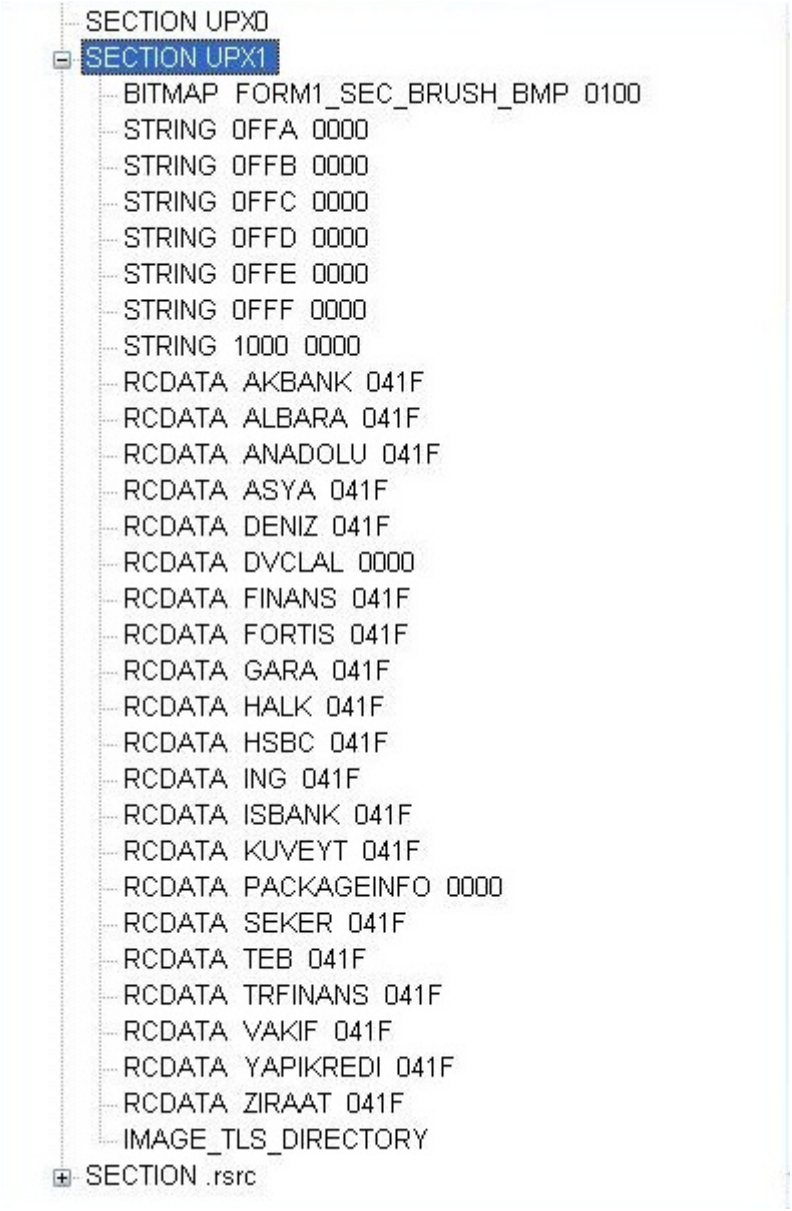
Dinamik olarak analiz ettiğimde ise;

- Çalıştırılır çalıştırılmaz windows\system32 klasörü altında javascheds.exe adında bir dosya, windows\system32\drivers klasörü altında ise ie_plugin.exe adında başka bir dosya oluşturduğunu,
- Windows\system32\drivers klasörü altında security adında gizli bir klasör oluşturarak içine 19 tane bankanın logosunu resim dosyası olarak kayıt ettiğini,
- Tuş kayıt bilgilerini C:\WINDOWS\system32\wins\syskl32.sys dosyasına kayıt ettiğini,
- İnternet bankacılığına giriş esnasında aldığı ekran görüntülerini C:\WINDOWS\system32\wins\setup klasörü altına kayıt ettiğini,
- ie_plugin.exe dosyasının UPX ile paketlenmiş olduğunu,
- DDE yöntemi ile bu 19 bankaya ait internet bankacılığı adreslerini izlediğini ve bu adreslere girilmesi durumunda TCKN ve cep telefonu bilgisi toplayan ve ilgili bankanın logosunu içeren bir pencere oluşturduğunu, tuş kaydı yaptığını ve ekran görüntüsü aldığını
- Güvenlik kalkanı ve güvenli girişi devre dışı bıraktığını,
- Sadece internet explorer ve firefox internet tarayıcılarını desteklediğini,
- Kayıt altına aldığı ekran görüntülerini ve tuş kayıtlarını ftp.my3gb.com sunucusuna göndermeye çalıştığını (ftp şifresi değiştiği ve my3gb yöneticileri tarafından hesap silindiği için sunucu adını ifşa ediyorum),
- TCKN bilgisi aldığı ekranda tckn algoritmasından faydalanarak doğrulama yaptığını ve hatalı tckn girilmesi durumunda hata mesajı çıkarttığını,
- Startup klasörüne SunJavaUpdateSched kısayolu oluşturduğunu,

- Trojan’da bug olduğunu, firefox.exe dosyasını ortam değişkenlerinden (environment variable) PATH değişkeninde yer alan tüm klasörlerde teker teker aradığını fakat hiç bir zaman bulamayacağını çünkü firefox’un kurulum esnasında klasör bilgisini PATH değişkenine eklemediğini, sürekli arama işlemi gerçekleştirmesi nedeniyle yüksek CPU tüketimine yol açtığını :p
- Bankalara ilave olarak PTT, Paypal ve bir hacking forumuna giriş esnasında ekran görüntüleri aldığını,
- 10 Aralık 2009 tarihinde analiz ettiğim zararlı yazılımın yeni bir varyantı olduğunu söyleyebilirim.

Güvenli girişi kaldırma girişimleri:
cmd.exe + command.com /c regsvr32 /u /s %WINDIR%/Downloaded Program Files/tebedit.ocx

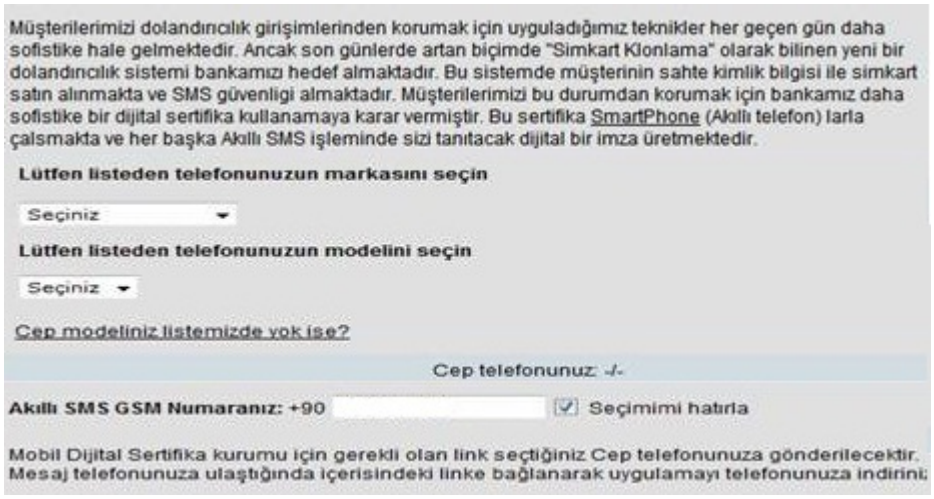
Güvenlik kalkanını kaldırma girişimleri:
cmd.exe + command.com /c regsvr32 /u /s %WINDIR%/Downloaded Program Files/JaguarEditControl.dll
cmd.exe + command.com /c regsvr32 /u /s %WINDIR%/Downloaded Program Files/JaguarEdit4ISB.dl



Efsane Zeus trojanına gelecek olursam elimde analiz edebilecek bir numune olmadığı için duyduklarımı ve gördüklerimi sizinle paylaşabilirim.

Bana “cep telefonuna bulaşan bir trojan varmış” diye söylediklerinde hemen aklıma bunun man in the mobile yapabilen Zeus trojanı olduğu geldi ve konuyla ilgili biraz daha bilgi edindiğimde bulaşma yönteminin de aynı olduğu öğrendim. Kullanıcıdan cep telefonu numarası, marka ve model alınıyor ve daha sonrasında sms ile bir web adresi gönderiliyor ve kullanıcı bu adresteki zararlı yazılımı yükler yüklemez artık cep telefonuna gelen SMSler (amaç internet bankacılığına giriş ve işlemler esnasında kullanılan SMS kodunu çalmak) gizlice (sms geldiği zaman cep telefonu size haber vermiyor) art niyetli kişilere gönderiliyordu. Buraya kadar herşey normaldi fakat ne zaman ki Zeus bulaşmış bir kullanıcıya ait ekran görüntüsü gördüm o zaman gözlerime inanamadım çünkü basit bir html injection ile sunucudan gelen yanıta bir form eklendiğini düşünürken çok farklı bir sahne ile karşılaştım. Aklınızda

canlandırabilmeniz adına her zaman girmiş olduğunuz internet bankacılığı uygulamasını düşünün ve girer girmez tasarım aynı, tüm menüler yerli yerinde, butonlar, font herşey orjinali ile aynı tek fark yeni bir mesaj ile karşılaşıyorsunuz. Mesajın içeriği oldukça başarılı kısaca sizi dolandırıcılıktan koruyacağını vaad eden bir sertifikayı cep telefonunuza yüklemeniz konusunda kandırmaya çalışıyor. Mesajı okuduğunuz zaman yazım hataları ve düşük cümleler sadece sizde şüphe uyandırıyor. Orjinal ekran görüntüsünü etik açıdan paylaşmam doğru olmayacağı için sadece mesajı sizlerle paylaşıyorum.



Açıkçası insan bu mesajı okuduktan sonra “vay canına beni bile kandırırdı” diye düşünmeden edemiyor. Zeus’un MIB yöntemini kullanan sürümünün yurt dışında keşfedilmesinin üzerinden daha 1 ay geçmeden bu kadar kısa bir süre içinde Türkiye’de ortaya çıkmasını beklemiyordum. Tüm bankaların SMS OTP kullandığı günümüzde umarım ilerleyen zamanlarda çok daha fazla banka müşterisini hedef alan bir trojan ile karşılaşmayız.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.