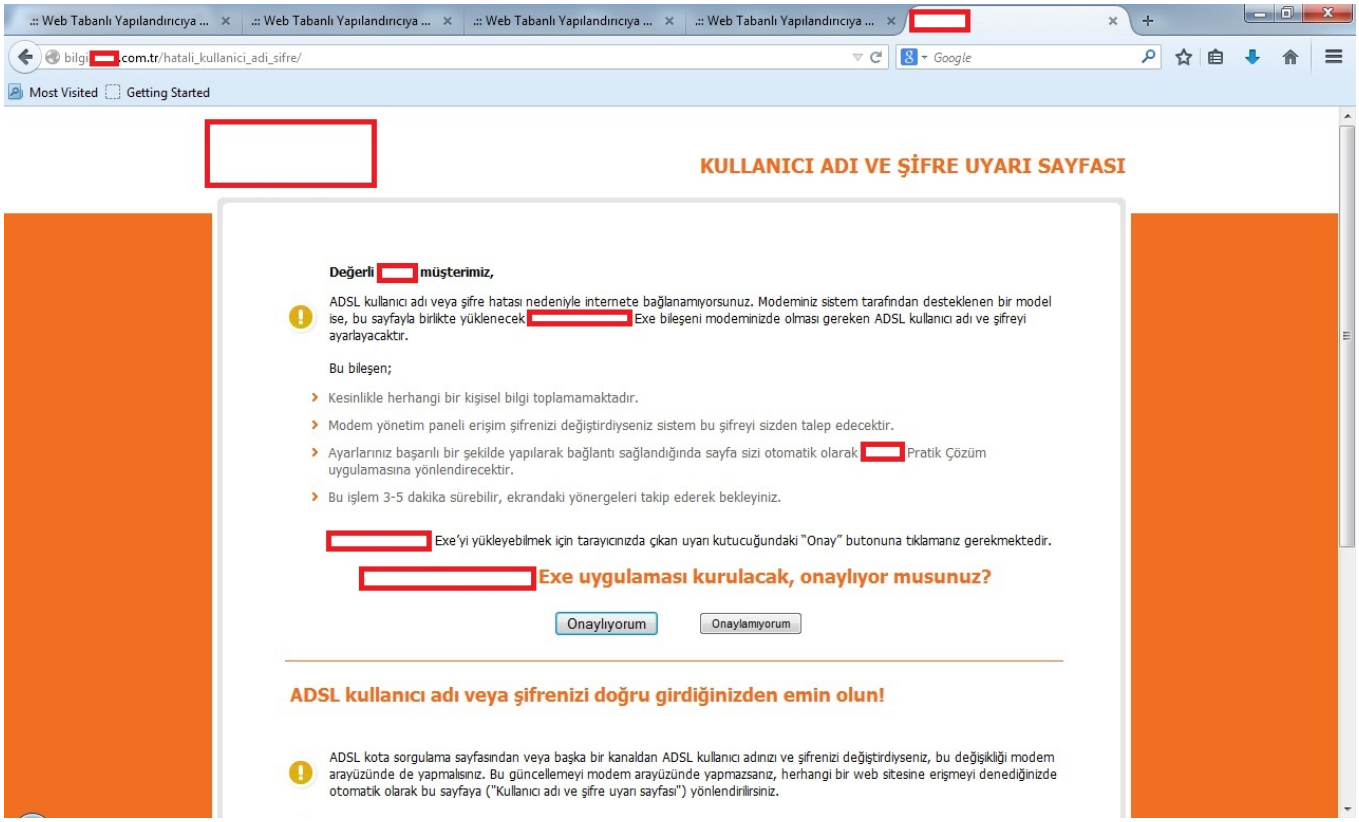
Kullanıcı Dostluğu vs Kullanıcı Güvenliği

written by Mert SARICA | 1 August 2014

Hemen hemen her bilişim güvenliği uzmanı (janjanlı adıyla siber güvenlik uzmanı) çalışma hayatı boyunca ilettiği güvenlik gereksinimleri, aksiyonlar nedeniyle şu cümleleri en az bir defa duymuştur, “Bu zamana kadar başımıza ne geldi ki ?”, “Buna gerçekten gerek var mı ?” Bu yaklaşımın aslında bu zamana kadar trafik kazası yapmamış bir kişinin aracındaki güvenlik donanımını sorgulamasından pek bir farkı yoktur. Bu hava yastığına gerçekten gerek var mı ? Bu emniyet kemerini takmasam olur mu ? Rekabetçi bir ortamda zaman zaman geliştirilmesi talep edilen güvenlik kontrolleri, alınması gereken güvenlik önlemleri, iş birimleri tarafından maliyet ve süre arttıran adımlar olarak görülebilmektedir. Kimi zaman ise mevcut güvenlik kontrolleri, müşteri memnuniyetini ve kullanım kolaylığını arttırma adına isteyerek veya istemeden zayıflatılabilmektedir. Özellikle bu tür zayıf noktalara şifremi hatırla, şifremi unuttum gibi sayfalarda rastlanabilmektedir.

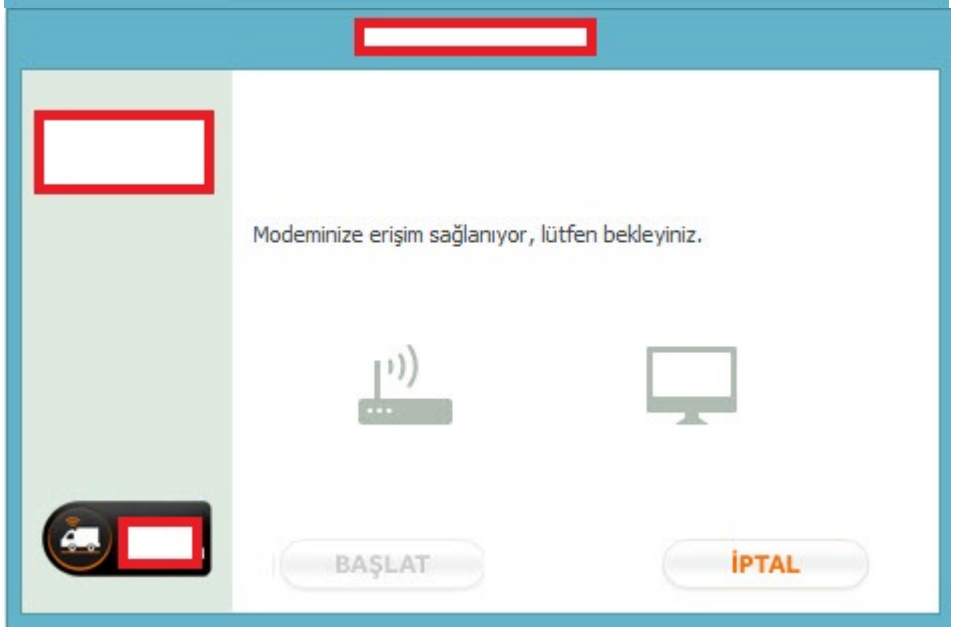
Hatırlayacağınız üzere geçtiğimiz yazımda, bir sohbet üzerine incelemeye başladığım modemim üzerinde güvenlik adına sıkıntı yaratabilecek bazı tespitlerimi paylaşmıştım. Bu yazımda da, modemim üzerinde çalışmalar yaparken tesadüfen karşılaştığım ve internet hizmeti aldığım internet servis sağlayıcısı (ISS) ile paylaştığım bir güvenlik zafiyetini, güvenlik farkındalığını arttırmak amacıyla sizlerle paylaşma kararı aldım.

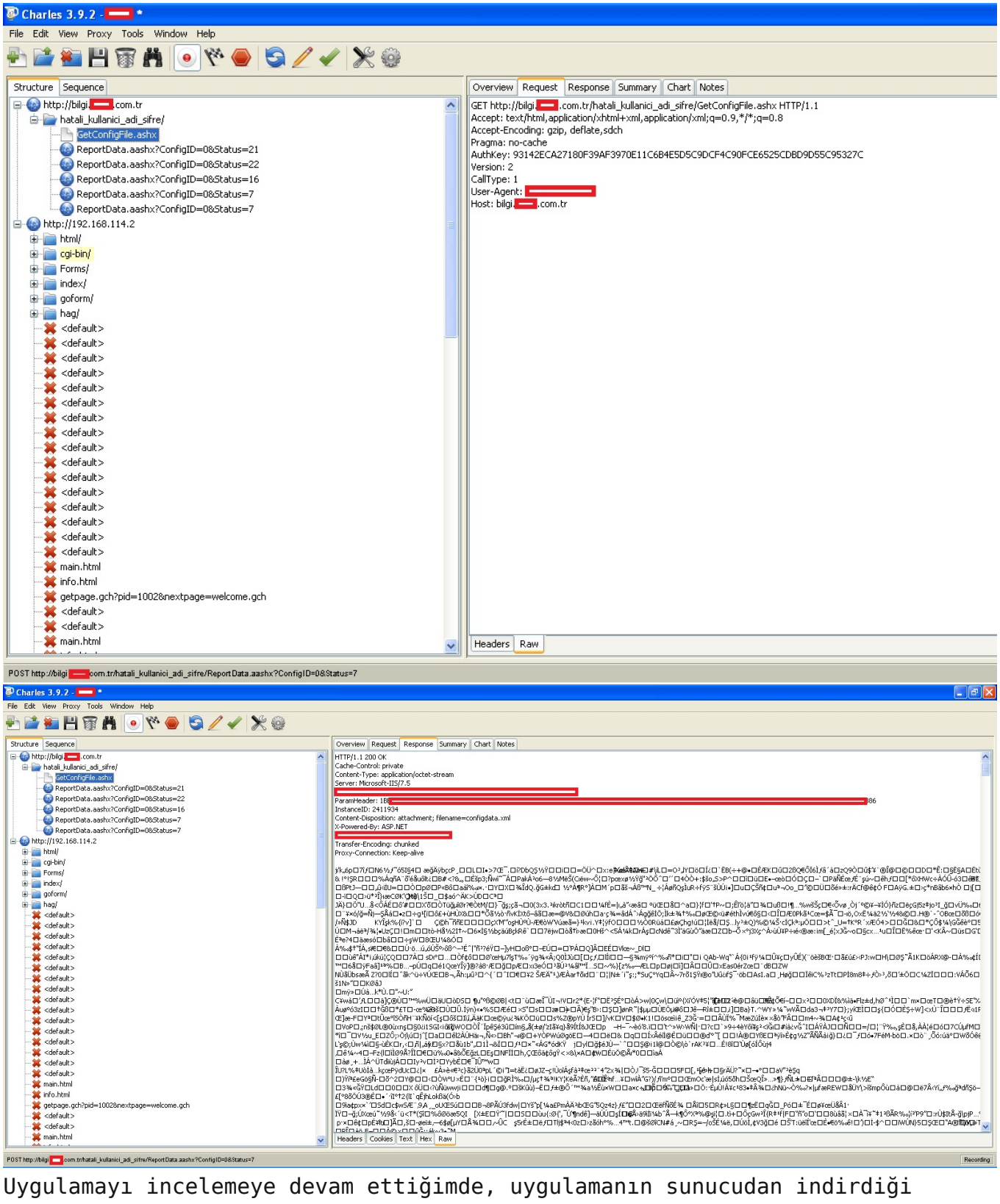
Çalışmalar esnasında modemi fabrika ayarlarına döndürdüğümde ISS’in beni şifre unuttum sayfasına yönlendirdiğini gördüm. Bu sayfada, ISS’in hazırlamış olduğu uygulamayı indirip, çalıştırmam durumunda, modemimin ADSL kullanıcı adı ve şifre bilgilerimin bu uygulama tarafından otomatik olarak modeme girileceği bilgisine yer veriliyordu.



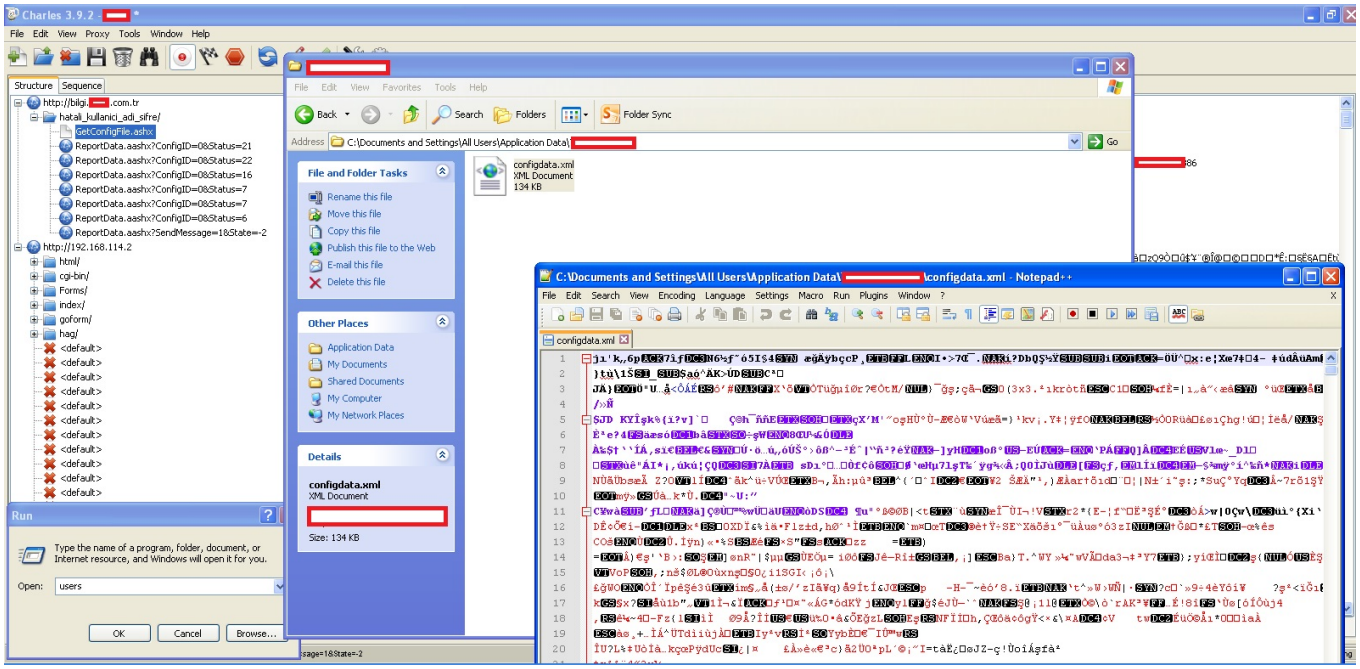
Yazımın başında da belirttiğim gibi bu tür otomatik şifre hatırlama, şifre girme gibi kullanıcı dostu araçlar, güvenli tasarlanmadığı taktirde güvenlik zafiyetlerine yol açabildiği için uygulamayı sistemime indirip, Immunity Debugger ve Charles Proxy araçları ile kısaca incelemeye karar verdim. Uygulamayı çalıştırdıktan sonra ilk olarak Charles Proxy aracı ile ağ trafiğini incelediğimde, uygulamanın bilgi.xxxxx.com.tr sunucusu ile haberleştiğini ve bu sunucudan şifreli bir içerik aldığını gördüm. Uygulama üzerinden Başlat butonuna bastıktan sonra ise uygulamanın ISS'in hediye olarak verdiği belli başlı marka, model modemlerin yönetici (admin) arayüzüne varsayılan (default) kullanıcı adı ve şifreler ile bağlanmaya çalıştığını gördüm. Yönetici paneline başarıyla giriş yapamadığı taktirde ise doğru kullanıcı adımı ve şifremi girmemi istiyordu.


Bu uygulamanın amacı modeminize ADSL Kullanıcı Adı ve Şifrenizi otomatik olarak ayarlamaktır.
Çalıştırmak için Başlat'a tıklayınız.
BAŞLAT
KAPAT


Modeminize erişim sağlanıyor, lütfen bekleyiniz.
BAŞLAT
İPTAL



Uygulamayı incelemeye devam ettiğimde, uygulamanın sunucudan indirdiği şifreli içeriği, dosya sistemi üzerinde configdata.xml adı altında bir dosyaya şifreli olarak kaydettiğini gördüm.

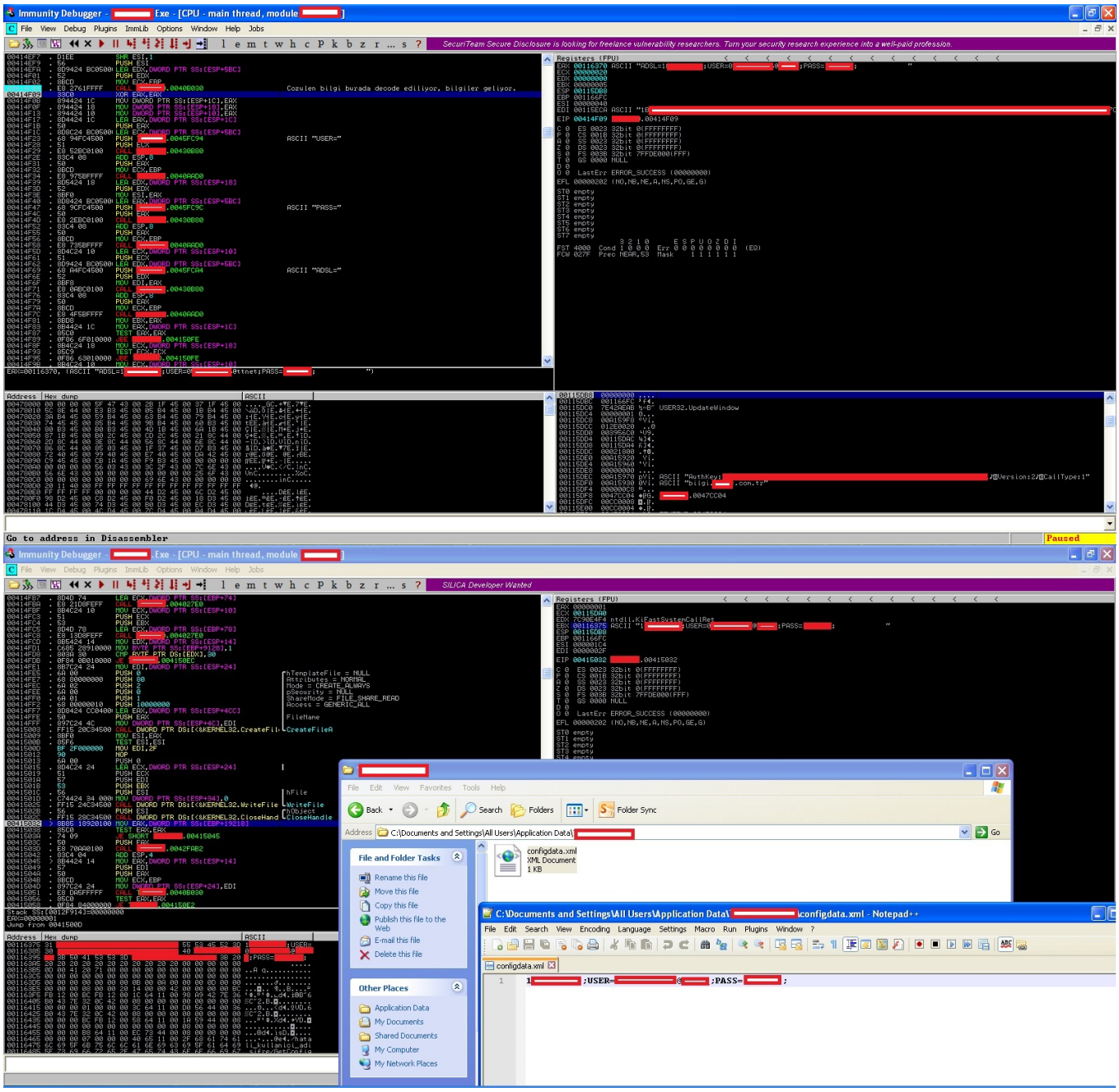


Bu uygulamanın doğru ADSL kullanıcı adı ve şifremi nasıl indirdiğini ve bu bilginin bu şifreli dosya içinde yer alıp almadığını öğrenmek için uygulamayı Immunity Debugger ile incelemeye başladım. Web trafiği ile ilgili fonksiyonları biraz inceledikten sonra indirilen bu şifreli içeriğin aslında hangi marka model modemlere, hangi varsayılan yönetici (admin) kullanıcı adı ve şifre ile bağlanacağı bilgisi olduğunu gördüm. ADSL kullanıcı adım ve şifrem ile ilgili olan fonksiyonu aramaya devam ederken çok geçmeden sunucudan şifreli bilgiyi alan ilgili fonksiyonu buldum. İncelemem sonucunda, ADSL kullanıcı adımın ve şifremin, uygulama tarafından çağrılan GetConfigFile.ashx sayfasına, sunucu tarafından dönülen yanıtta yer alan ParamHeader başlığında şifreli olarak yer aldığını gördüm. İlk dikkatimi çeken sıkıntılı nokta, uygulamayı çalıştırıp Başlat butonuna basmasam bile, bu uygulama gidip bu isteği otomatik olarak sunucuya gönderiyor ve şifreli ADSL kullanıcı adı ve şifremi sunucudan alıyordu. Bu durumu, PİN/Şifre koruması devrede olmayan cep telefonunuzu çaldırdığınızda, art niyetli kişinin cep telefonunuzdan bankanızın çağrı merkezini arayıp herhangi bir doğrulama adımından geçmeden kredi kartı veya bankamatik kartınızın PİN'ini öğrenebilmesine benzettim.

Sistemime bulaşmış bir zararlı yazılımın, şifreli ADSL kullanıcı adı ve şifremin açık/şifresiz haline ulaşmasının ne kadar kolay olup olamayacağını öğrenmek için bu defa uygulamanın aldığı şifreli bilgiyi çözen (decrypt) ilgili fonksiyonu aramaya başladım ve çok geçmeden fonksiyonu buldum. Zararlı yazılımın şifremin açık halini ele geçirmesinin ne kadar kolay olabileceğini anlamak için izleyebileceği yollar üzerine biraz düşünmeye başladım. Aklıma gelen ilk üç yol; 1-) Şifre çözme fonksiyonunun algoritmasını anlayıp, başka

bir programlama diline çevirecek 2-) Code cave yöntemi ile akışı kodun farklı bir yerinde oluşturduğu koda gönderecek 3-) Uygulama üzerinde diske veri yazmak için kullanılan API'ler (WriteFile, CreateFile) var ise uygulama yamalanarak (patch), şifrenin çözülmüş halinin bu API'lere yönlendirilecek ve şifreli bilgiler açık olan diske yazılacak

Amacım olası güvenlik zafiyetini tespit etmek ve durumu ISS'e bildirmek olduğu için kolay yolu yani 3. yolu seçmeye karar verdim. Uygulamanın sunucudan şifreli bilgileri aldığını ve bunu configdata.xml dosyasına kaydettiğini bildiğim için şifresi çözülen bu bilgileri configdata.xml dosyasına yazan fonksiyona yönlendirdim ve uygulamayı bu haliyle diske kaydettim. Yamalanmış uygulamayı çalıştırdığımda artık uygulama şifreli bilgileri sunucudan alıyor ve diske kaydediyordu.



ISS tarafından kullanıcı dostu olarak müşterilerinin hizmetine sunulan bu uygulama aslında istemeden de olsa art niyetli kişilerin (örneğin ortak şifre ile cafeden kablosuz ağ kullanan bir kişi) veya zararlı yazılımların kullanıcının ADSL hizmet numarası, adsl kullanıcı adı ve şifresine kolaylıkla ulaşabilmesini sağlıyordu. Vakit geçmeden, POC için çektiğim video da dahil olmak üzere elimdeki tüm bilgileri ISS ile paylaşarak zafiyet bildiriminde bulundum ve bir zafiyet daha art niyetli kişiler tarafından kötüye kullanılmadan önce tespit edilmiş oldu.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.