

Kullanıcı Dostluğu vs Kullanıcı Güvenliđi

written by Mert SARICA | 1 August 2014

Hemen hemen her biliřim güvenliđi uzmanı (janjanlı adıyla siber güvenlik uzmanı) alıřma hayatı boyunca ilettiđi güvenlik gereksinimleri, aksiyonlar nedeniyle řu cümleleri en az bir defa duymuřtur, “Bu zamana kadar bařımıza ne geldi ki?”, “Buna gerekten gerek var mı?” Bu yaklařımın aslında bu zamana kadar trafik kazası yapmamıř bir kiřinin aracındaki güvenlik donanımını sorgulamasından pek bir farkı yoktur. Bu hava yastıđına gerekten gerek var mı? Bu emniyet kemerini takmasam olur mu? Rekabeti bir ortamda zaman zaman geliřtirilmesi talep edilen güvenlik kontrolleri, alınması gereken güvenlik önlemleri, iř birimleri tarafından maliyet ve süre arttıran adımlar olarak görülebilmektedir. Kimi zaman ise mevcut güvenlik kontrolleri, müřteri memnuniyetini ve kullanım kolaylıđını arttırma adına isteyerek veya istemeden zayıflatılabilmektedir. Özellikle bu tür zayıf noktalara řifremi hatırla, řifremi unuttum gibi sayfalarda rastlanabilmektedir.

Hatırlayacađınız üzere getiđimiz yazımda, bir sohbet üzerine incelemeye bařladıđım modemim üzerinde güvenlik adına sıkıntı yaratabilecek bazı tespitlerimi paylařmıřtım. Bu yazımda da, modemim üzerinde alıřmalar yaparken tesadüfen karřılařtıđım ve internet hizmeti aldıđım internet servis sađlayıcısı (ISS) ile paylařtıđım bir güvenlik zafiyetini, güvenlik farkındalıđını arttırmak amacıyla sizlerle paylařma kararı aldım.

alıřmalar esnasında modemi fabrika ayarlarına döndürdüđümde ISS’in beni řifre unuttum sayfasına yönlendirdiđini gördüm. Bu sayfada, ISS’in hazırlamıř olduđu uygulamayı indirip, alıřtırmam durumunda, modemimin ADSL kullanıcı adı ve řifre bilgilerimin bu uygulama tarafından otomatik olarak modeme girileceđi bilgisine yer veriliyordu.

Web Tabanlı Yapılandırıcıya ... x Web Tabanlı Yapılandırıcıya ... x Web Tabanlı Yapılandırıcıya ... x Web Tabanlı Yapılandırıcıya ... x [redacted] x +

bilgi [redacted].com.tr/hatali_kullanici_adi_sifre/ Google

Most Visited Getting Started

KULLANICI ADI VE ŞİFRE UYARI SAYFASI

Değerli [redacted] müşterimiz,

ADSL kullanıcı adı veya şifre hatası nedeniyle internete bağlanamıyorsunuz. Modeminiz sistem tarafından desteklenen bir model ise, bu sayfaya birlikte yüklenecek [redacted] Exe bileşeni modeminizde olması gereken ADSL kullanıcı adı ve şifreyi ayarlayacaktır.

Bu bileşen;

- Kesinlikle herhangi bir kişisel bilgi toplamamaktadır.
- Modem yönetim paneli erişim şifrenizi değiştirdiyse sistem bu şifreyi sizden talep edecektir.
- Ayarlarınız başarılı bir şekilde yapılarak bağlantı sağlandığında sayfa sizi otomatik olarak [redacted] Pratik Çözüm uygulamasına yönlendirecektir.
- Bu işlem 3-5 dakika sürebilir, ekrandaki yönergeleri takip ederek bekleyiniz.

[redacted] Exe'yi yükleyebilmek için tarayıcınızda çıkan uyarı kutucuğundaki "Onay" butonuna tıklamanız gerekmektedir.

[redacted] Exe uygulaması kurulacak, onaylıyor musunuz?

ADSL kullanıcı adı veya şifrenizi doğru girdiğinizden emin olun!

ADSL kota sorgulama sayfasından veya başka bir kanaldan ADSL kullanıcı adınızı ve şifrenizi değiştirdiyse, bu değişikliği modem arayüzünde de yapmalısınız. Bu güncellemeyi modem arayüzünde yapmazsanız, herhangi bir web sitesine erişmeyi denediğinizde otomatik olarak bu sayfaya ("Kullanıcı adı ve şifre uyarı sayfası") yönlendirilirsiniz.

Yazımın başında da belirttiğim gibi bu tür otomatik şifre hatırlama, şifre girme gibi kullanıcı dostu araçlar, güvenli tasarlanmadığı takdirde 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 takdirde ise doğru kullanıcı adımı ve şifremi girmemi istiyordu.

[Redacted]

[Redacted]

Bu uygulamanın amacı modeminize [Redacted] ADSL Kullanıcı Adı ve Şifrenizi otomatik olarak ayarlamaktır.

Çalıştırmak için Başlat'a tıklayınız.



BAŞLAT

KAPAT

[Redacted]

[Redacted]

Modeminize erişim sağlanıyor, lütfen bekleyiniz.



BAŞLAT

İPTAL

Charles 3.9.2

Structure Sequence

- http://bilgi.com.tr
 - hatali_kullanici_adi_sifre/
 - GetConfigFile.ashx
 - ReportData.ashx?ConfigID=0&Status=21
 - ReportData.ashx?ConfigID=0&Status=22
 - ReportData.ashx?ConfigID=0&Status=16
 - ReportData.ashx?ConfigID=0&Status=7
 - ReportData.ashx?ConfigID=0&Status=7
 - http://192.168.114.2
 - html/
 - cgi-bin/
 - Forms/
 - index/
 - goform/
 - hag/
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - main.html
 - info.html
 - getPage.gch?pid=1002&nextpage=welcome.gch
 - <default>
 - <default>
 - main.html

Overview Request Response Summary Chart Notes

GET http://bilgi.com.tr/hatali_kullanici_adi_sifre/GetConfigFile.ashx HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip, deflate, sdch
Pragma: no-cache
AuthKey: 93142ECA27180F39AF3970E11C6B4E5D5C9DC490FC6525CDB9D55C95327C
Version: 2
CallType: 1
User-Agent: [REDACTED]
Host: bilgi.com.tr

Headers Raw

Charles 3.9.2

Structure Sequence

- http://bilgi.com.tr
 - hatali_kullanici_adi_sifre/
 - ReportData.ashx?ConfigID=0&Status=21
 - ReportData.ashx?ConfigID=0&Status=22
 - ReportData.ashx?ConfigID=0&Status=16
 - ReportData.ashx?ConfigID=0&Status=7
 - ReportData.ashx?ConfigID=0&Status=7
 - http://192.168.114.2
 - html/
 - cgi-bin/
 - Forms/
 - index/
 - goform/
 - hag/
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - <default>
 - main.html
 - info.html
 - getPage.gch?pid=1002&nextpage=welcome.gch
 - <default>
 - <default>
 - main.html

Overview Request Response Summary Chart Notes

POST http://bilgi.com.tr/hatali_kullanici_adi_sifre/ReportData.ashx?ConfigID=0&Status=7

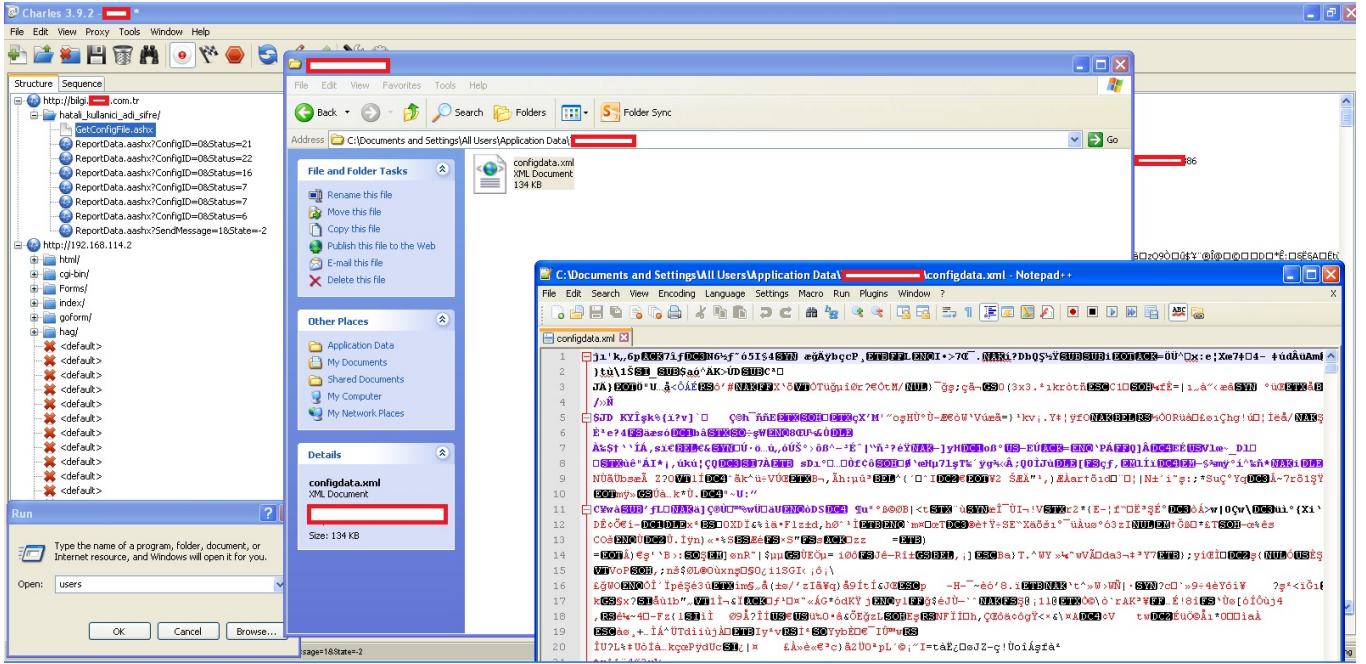
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/octet-stream
Server: Microsoft-IIS/7.5
Instant: 24/11/2014
Content-Disposition: attachment; filename=configdata.xml
X-Powered-By: ASP.NET

Transfer-Encoding: chunked
Proxy-Connection: keep-alive

[REDACTED]

Headers (Cookies) Text | Hex | Raw

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

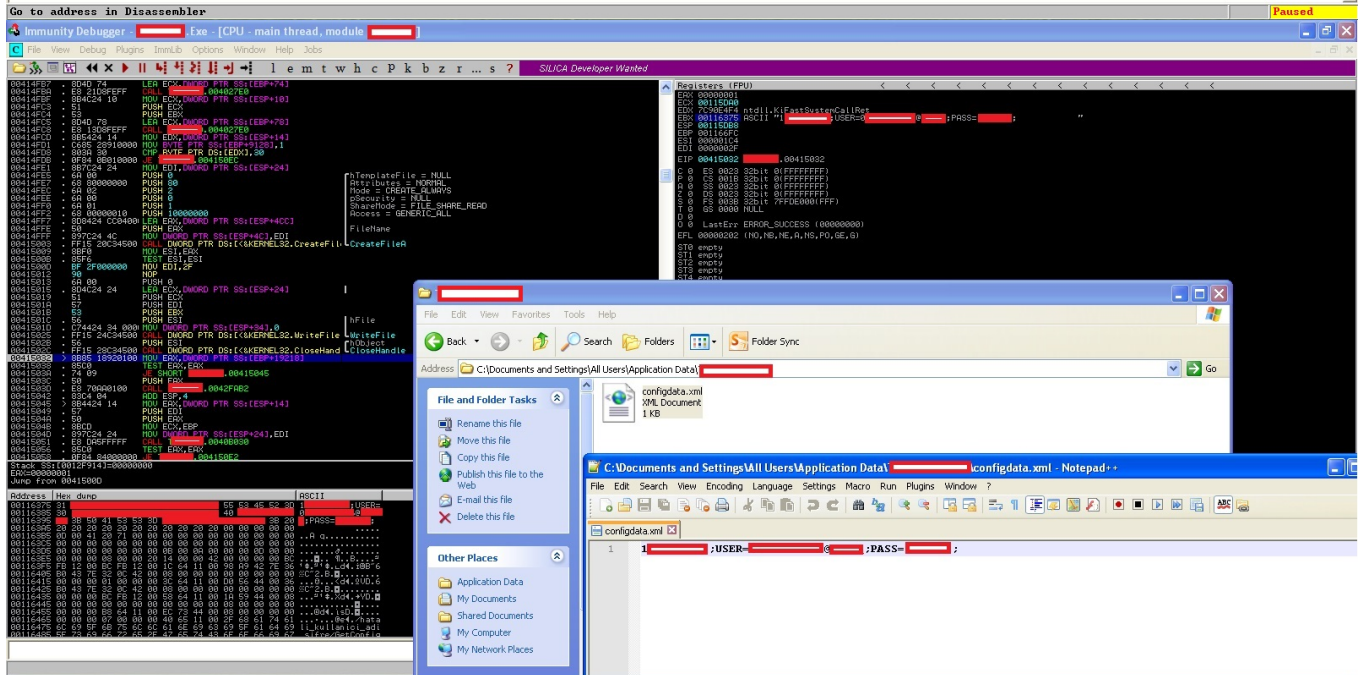
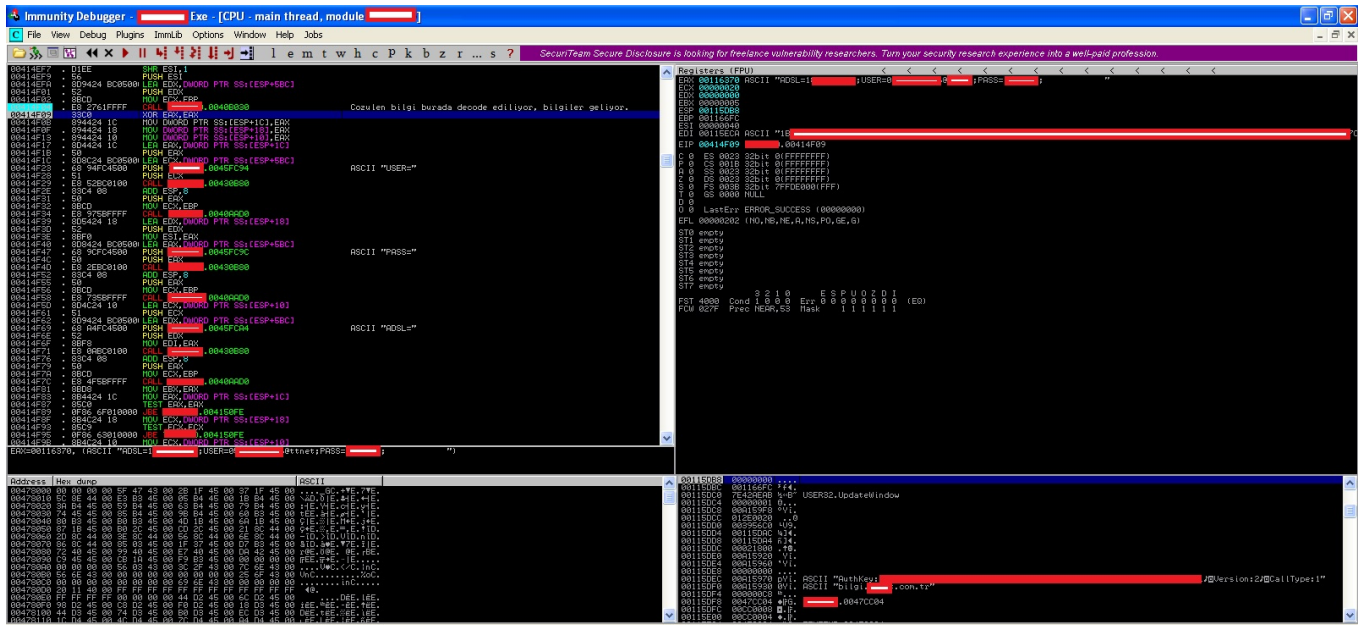


Bu uygulamanın doğru ADSL kullanıcı adı ve şifremini nasıl indirdiğini ve bu bilginin bu şifreli dosya içinde yer alıp almadığını öğrenmek için uygulamayı Immunity Debugger ile incelemeye başladım. Web trafiği ile ilgili fonksiyonları biraz inceledikten sonra indirilen bu şifreli içeriğin aslında hangi marka model modemlere, hangi varsayılan yönetici (admin) kullanıcı adı ve şifre ile bağlanacağı bilgisi olduğunu gördüm. ADSL kullanıcı adımı ve şifrem ile ilgili olan fonksiyonu devam ederken çok geçmeden sunucudan şifreli bilgiyi alan ilgili fonksiyonu buldum. İncelemem sonucunda, ADSL kullanıcı adı ve şifrem, uygulama tarafından çağrılan GetConfigFile.ashx sayfasına, sunucu tarafından dönen 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 şifremini 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 kartınızı PİN'ini öğrenebilmesine benzettim.

Sistemime bulaşmış bir zararlı yazılımın, şifreli ADSL kullanıcı adı ve şifremi açık/şifresiz haline ulaşmasının ne kadar kolay olup olmayacağını öğrenmek için bu defa uygulamanın aldığı şifreli bilgiyi çözen (decrypt) ilgili fonksiyonu aramaya başladım ve çok geçmeden fonksiyonu buldum. Zararlı yazılımın şifremi açık haline 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 buldum ve bir zafiyet daha art niyetli kişiler tarafından kötüye kullanılmadan önce tespit edilmiş oldu.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.