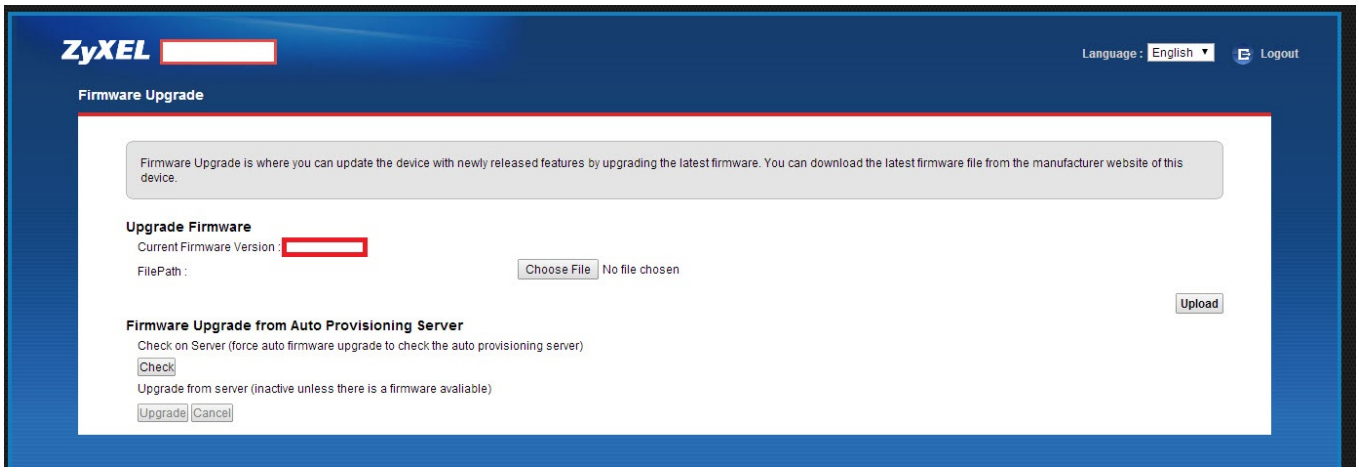
Hediye Modemler Ne Kadar Güvenli?

written by Mert SARICA | 1 July 2014

Bir öğle vakti iş arkadaşlarımla yürürken, internet servis sağlayıcılarının (ISS) müşterilerine dağıttığı modemlere ISS çalışanlarının uzaktan bağlanabileceği ile ilgili bir konu açılıverdi. Ben de cihaz yazılımının (firmware) güncellenmesi durumunda ISS'in modemlere nasıl erişim sağlayabileceklerini sorgularken, bir arkadaşım cihaz yazılımı güncellemesinin de ISSler'in sunucuları üzerinden gerçekleştiğini belirtti. NSA'in cihaz yazılımlarına (firmware) arka kapı yerleştirdiği, devletimizin ISSler üzerinden SSL trafiğin araya girilmesini planladığı şu günlerde, ISSler verdiği modemleri kullanmak ister istemez insanın aklında soru işaretlerine yol açıyordu. Bu zamana dek ISS'in hediye ettiği modemi kullanan ve bu konuyu irdelememiş bir güvenlik uzmanı olarak eve gider gitmez Zyxel marka modemime kısaca göz atmaya karar verdim.

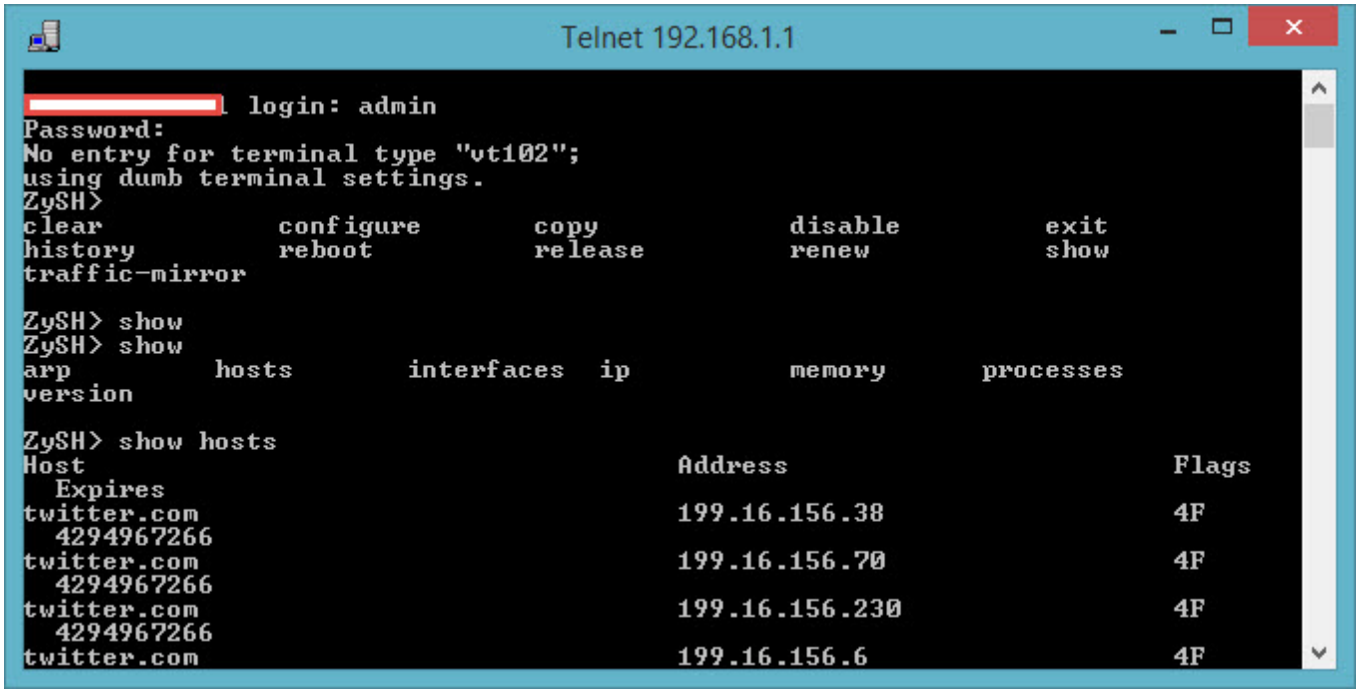
İlk yaptığım iş modemin web arayüzüne bağlanıp, yeni cihaz yazılımı kontrolünü gerçekleştirmek oldu fakat bu kontrolün Zyxel'in kendi resmi sunucularından mı yoksa ISS'in sunucularından mı gerçekleştirildiğini araştırmak oldu.



Web arayüzünden bununla ilgili edinilecek bilgi olmadığından ötürü bunun için ya modemin tüm trafiğini izleyecektim (sniff) ve ipucu elde etmeye çalışacaktım ya da modemin arabirimi (console) üzerinden komutlar ile bunu öğrenecektim. Kolay yoldan ilermeye karar vererek modeme telnet ile eriştim ve desteklediği komutları teker teker incelemeye başladım.

Sızma testi uzmanı olarak switch ve routerlar ile az çok haşır neşir olmuş

biri olarak dikkatimi ilk çeken show komutu oldu. Bu komutun çoğunlukla cihaz üzerindeki konfigürasyon bilgilerinin, anlık trafik bilgilerinin görüntülenmesi için kullanıldığını bildiğim için show hosts komutunu çalıştırdım ve ardından modemin o esnada iletişim kurduğu tüm adresleri görebildim.



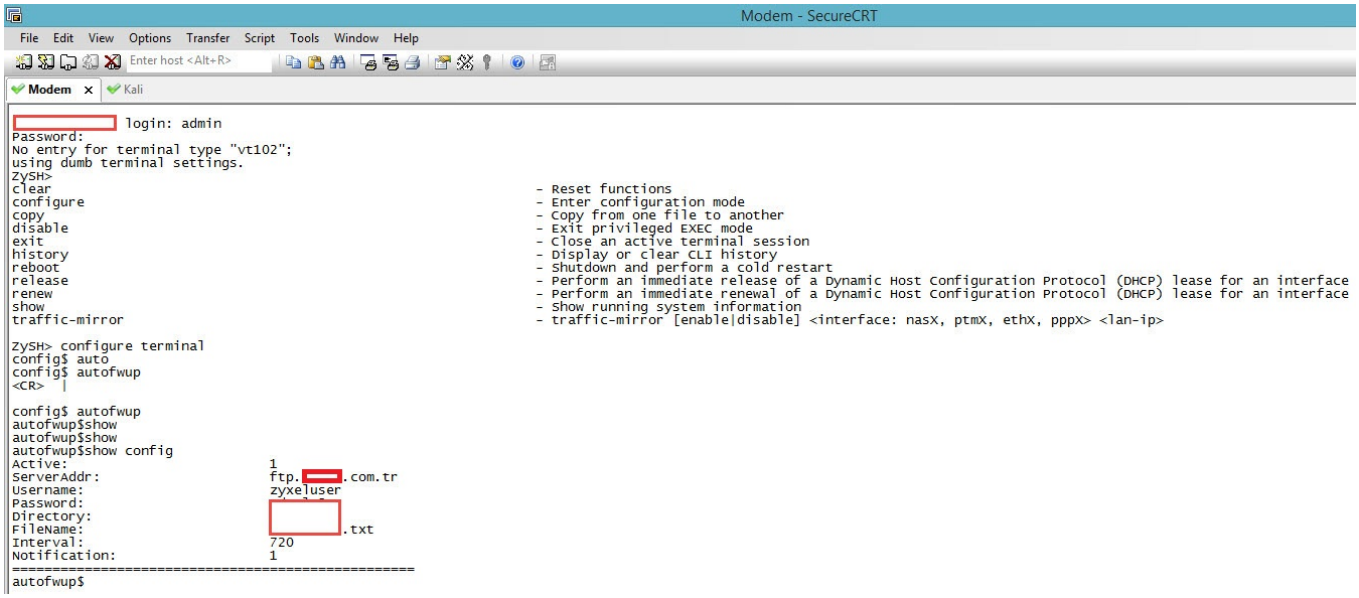
Amacım güncel cihaz yazılımının nereden kontrol edildiği bilgisini öğrenmek olduğu için, modemin web arayüzünden cihaz yazılımını kontrol et butonuna bastım ve ardından telnet arabirimi üzerinden show hosts komutunu çalıştırarak, cihaz yazılımının kontrol edildiği sunucuyu aramaya başladım. Çok geçmeden ftp.xxxxx.com.tr adresi dikkatimi çekti. FTP bilindiği üzere güvenli olmayan (kullanıcı adı ve şifre ağ üzerinden şifresiz olarak iletilmektedir) bir protokoldür. FTP iletişimini görünce aklıma hemen iki soru geldi ?

1- Trafiğinizi izleyen NSA, cihaz yazılımı kontrol butonuna basıldıktan sonra sunucudan size gelen cihaz yazılımını arka kapı yüklü olan bir yazılım ile değiştirebilir mi ?

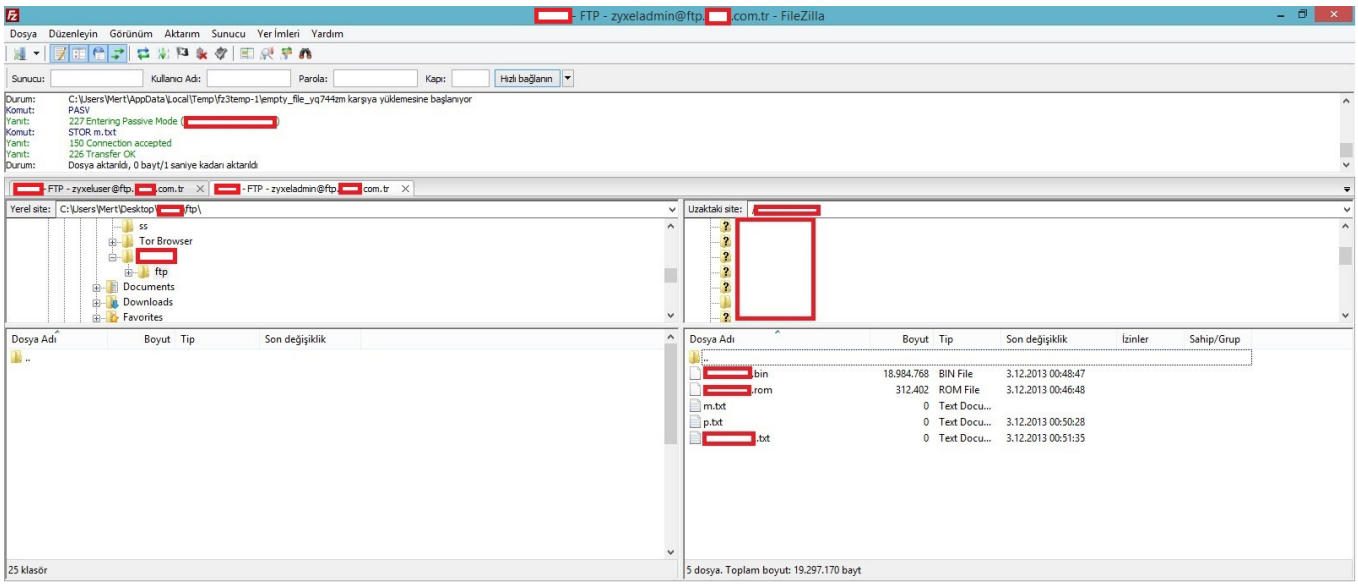
2- FTP kullanıcı adı ve şifresi modemin üzerinde tutulduğu için bunu ele geçiren NSA, bu kullanıcı adı ve şifre ile cihaz yazılımının bulunduğu sunucuya erişip, oradaki cihaz yazılımını arkakapı yüklü olan başka bir yazılım ile değiştirebilir mi ?

Bu sorulara yanıt aramak için FTP kullanıcı adı ve şifresini modem üzerinden öğrenmek için işe koyuldum. Yine tüm modem trafiğini izlemek yerine komutlar üzerinden ilerlemeye karar verdim. Çok geçmeden autofwup komutunun FTP

sunucusuna bağlanmak için gerekli bilgileri (kullanıcı adı: zyxeluser) gösterdiğini buldum.



Modemime verilen yetki dahilinde, bu kullanıcı adı ve şifre ile FTP sunucusuna bağlandığımda, bu sunucu üzerinde Zyxel marka modemlere ait olan cihaz yazılımlarının tutulduğunu gördüm. Bu kullanıcının sunucuya veri yazma yetkisi olup olmadığını görmek için sunucuya bir metin belgesi (m.txt) yükledim fakat yetkim olmadığı için hata aldım. Diğer cihaz yazılımlarının bulunduğu klasörlere göz attığımda, bazı dosyalar içinde modemlerin yönetici yetkisi (kullanıcı adı: zyxealadmin) ile bu sunucuya bağlanabildiklerini gördüm. Bu kullanıcı adı ve şifre ile FTP sunucusuna bağlanıp yine bir metin belgesini (m.txt) sunucuya yüklemeye çalıştığımda bu defa başarıyla yükleyebildiğimi farkettim. Bu durumda tüm cihaz yazılımlarını değiştirebilecek yetkiye sahiptim.



ISS'in müşterilerinin güvenliği adına hemen bu durumu ISS yetkilileri ile paylaşmaya (responsible disclosure) karar verdim. Paylaşımda bulunduktan kısa

bir süre içinde ISS yetkililerinden durumu araştırdıklarına dair bir yanıt geldi. Bir gün sonra ISS'ten gelen nihai yanıtta ise modemlerin cihaz yazılımı kontrolünü ve yüklemesini farklı bir yöntemle yaptığı, bunun yedek yöntem olduğu ve yedek olmasına rağmen FTP kullanıcı adı ve şifresinin yürürlükten kaldırıldığı bilgisi yer alıyordu. Buna ilave olarak cihaz yazılımları değiştirilse dahi, modemin olası bir değişikliğe karşı (muhtemelen cihaz yazılımları geliştirici tarafından imzalanıyor) yazılımı yüklemeden önce kontrol ettiği bilgisi paylaşılmıştı. (Kendilerine hem hızlı geri dönüş yaptıkları hem de aksiyon aldıkları için teşekkür etmeyi ihmal etmeyelim.)

Tabii bir güvenlik uzmanı olarak bu yanıtı okuduğumda aklıma aşağıdaki sorular geldi;

1- FTP üzerinden cihaz yazılımı güncellemesi yedek yöntem ise yazılımı kontrol et butonuna basıldığında neden birincil yöntem kullanılmıyordu ?
2- Sosyal mühendislik saldırısı ile hedef kullanıcıya bir e-posta gönderilse ve yeni güncelleme için bu botuna basın denilse ve öncesinde de bu FTP sunucusunda ilgili yazılım başka bir zararlı yazılım ile değiştirilse (imzalı olduğu düşünülse) modem yükleme yapmayacak mıydı ?
3- Zyxel marka modemler dışında diğer marka modemler de aynı şekilde FTP sunucusu üzerinden bu kontrolü yapıyor muydu ?
4- Cihaz yazılımı kontrolü, Zyxel marka modemler dışında diğer marka modemler tarafından da yapılıyor mu ?

Bu kısa süreli çalışma ile ISSler'in bize hediye etmiş olduğu ve üzerinde ISSler'e özel cihaz yazılımların çalıştığı modemleri kullanmadan önce iyi düşünmemiz gerektiğini öğrenmiş oldum.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.