İstemci Tarafındaki Zafiyetler

written by Mert SARICA | 2 June, 2010

Ağ ve uygulama seviyesinde konumlandırılan saldırı tespit sistemlerinin geçtiğimiz yıllara oranla daha etkili koruma mekanizmalarına sahip olmaları ve özellikle internete açık olan sunucuların konfigürasyon ve bağlantı noktaları düzeyinde sıkılaştırılıyor (harden) olmaları sunucular üzerindeki saldırı yüzeylerini azaltmaktadır. Buna ilaveten günümüzde artık çoğu işlemin istemci (client) tarafında gerçekleşiyor olması ve insanın doğası gereği bilgi güvenliğindeki en zayıf halka olması art niyetli kişilerin istemci uygulamalarını istismar etmeye yöneltmektedir. Örneğin internet üzerinden gerçekleşesen saldırılara karşı oldukça korunaklı bir sunucuyu ele geçirmek isteyen art niyetli bir kişinin sunucuyu ele geçirmek için harcayacağı efor ile bu sunucuya erişimi olan bir kullacının işletim sistemini ele geçirmeye harcayacağı efor arasında uçurum olabilir. Sunucuyu ele geçirmek için 3 farklı saldırı önleme mekanizmasını aşması gerekirken diğer türlü güvenlik zafiyetine sahip olan bir excel dosyasını kurbana göndermesi ve kurbanın bu dosyayı açması art niyetli kişiyi çok daha kısa sürede, kolay yoldan başarıya ulaştırabilir. Bu nedenden ötürü kullanıcıların bilgi güvenliği farkındalığını arttırmaya yönelik eğitimler, kurumlar için oldukça büyük önem arz etmektedir.

İstemci tarafındaki zafiyetlerin istismar edilmesi çoğu zaman yaması güncel olmayan bir uygulamadan kaynaklanabildiği gibi mimari olarak gerekli kontrolleri uygulamayan bir uygulamadan da kaynaklanıyor olabilir. Örneğin kullanıcı işletim sistemi üzerinde yüklü olan bir uygulama haberleşme esnasında SSL doğrulaması yapmıyor ve sunucuyu dijital imza ile doğrulamıyorsa, uygulama üzerinden gerçekleşen otomatik güncelleme özelliğinin kullanıcı ile sunucu arasına giren art niyetli kişi tarafından kötüye kullanılması (evilgrade saldırısı) ile son bulabilir. Bu haftaki yazımda aynı bu şekilde bir soruna yol açabilen Türk Telekom firmasının Wirofon uygulamasında keşfetmiş olduğum güvenlik açığından kısaca bahsedeceğim.

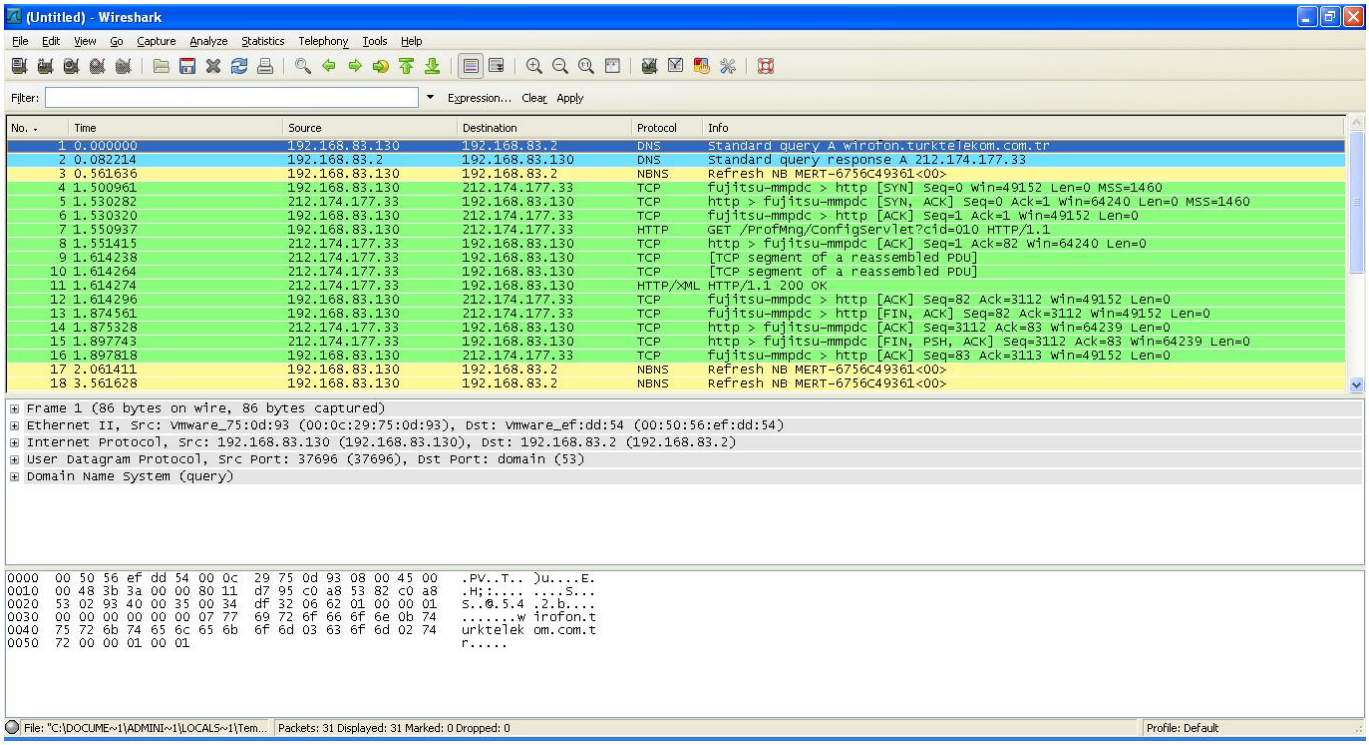
Öncelikle bu konunun responsible disclosure adına Türk Telekom yetkililerine iletildiğini ve kendilerinin benimle çok kısa süre içerisinde iletişime geçerek konuya profesyönelce yaklaştıklarını ve bilgi edindiğini söylemek isterim. Akabinde kendileri ile iletişime geçmeye çalışarak konu ile ilgili Wirofon uygulamasında bir güvenlik iyileştirmesi yapılıp yapılmayacağı konusunda bilgi edinme çabalarımın sonuçsuz kaldığınıda üzülerek belirtmek isterim. Çabalarımın sonuçsuz kalması neticesinde insanları bu zafiyet konusunda bilgilendirmek, olası istismar girişimleri konusunda dikkatli olmalarını sağlamak ve dolaylı olarak Türk Telekom'un bu zafiyeti ortadan kaldırmasını sağlamak amacıyla yazımda bu konuya yer vermekteyim.

Öncelikle işe Wirofon uygulamasını kurmak ve daha sonrasında trafiği izlemekle başladım. Malum aradaki sunucu ile uygulama arasındaki trafik SSL olduğu için araya girmek uygulama seviyesi haricinde pek mümkün değildi bu nedenle hindi gibi düşünürken bir anda Wirofon uygulaması ile aynı klasörde

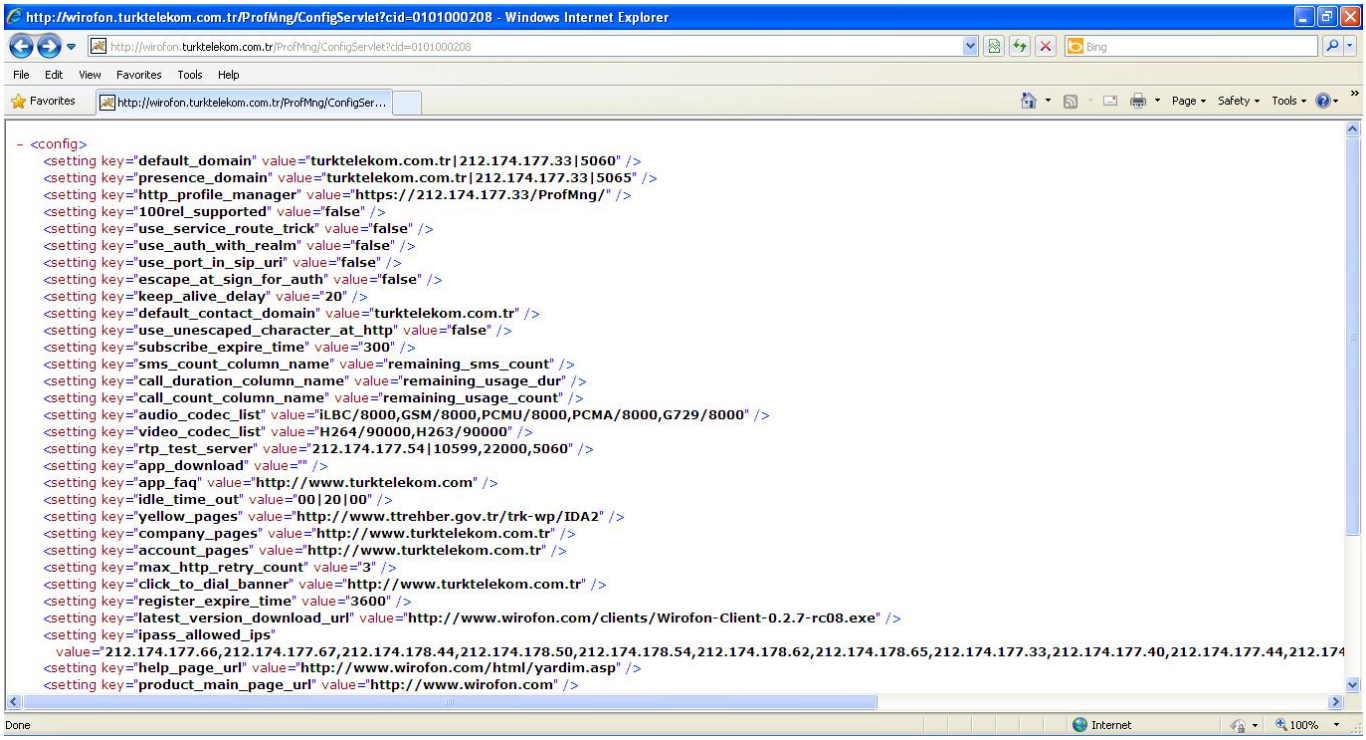
yer alan konfigürasyon dosyalarına göz atmaya karar verdim ve init.properties dosyası içerisinde yer alan satır dikkatimi çekti.

```
current_version = 1.1.0.2.7
config_url = https://wirofon.turktelekom.com.tr/ProfMng/ConfigServlet
domain_servlet =
```

Kısa yoldan şifresiz haberleşmenin gerçekleşip gerçekleşmediğini teyit etmek için https yerine http://wirofon.turktelekom.com.tr/ProfMng/ConfigServlet adresine gitmeye çalıştığımda herhangi bir hata ile karşılaşmadığımı farkettim. Bu sayede konfigürasyon dosyasındaki **config_url** parametresinde yer alan adresi https'den http'ye çevirmem ile trafiğin şifresiz olarak gerçekleşmesini ve bu sayede trafiği izleyebilmeyi umuyordumki çok geçmeden umduğumu bulabildim.



Trafiği analiz ettikten sonra Wirofon uygulamasının çalıştırıldıktan hemen sonra ConfigServlet dosyasına istekte bulunduğunu ve sunucudan gelen yanıtta yer alan konfigürasyon parametrelerine göre konfigürasyonunu güncellediğini farkettim.



Parametreleri teker teker incelediğimde en çok dikkatimi **latest_version_download_url** parametresi çekmişti çünkü eğer ben art niyetli biri olsaydım yapacağım ilk iş bu adresi değiştirerek kullanıcıyı zararlı yazılımın bulunduğu adrese yönlendirmek ve kullanıcının bu dosyayı çalıştırmasını beklemek olurdu.

Sanal makina üzerinde MITM saldırısı gerçekleştirerek **latest_version_download_url** parametresini değiştirdiğimde program üzerinde yeni bir sürümün çıktığını belirten herhangi bir uyarı mesajı ile karşılaşmadım bunun üzerine otomatik güncellemeyi tetikleyebilecek başka bir parametrenin daha olabileceğini düşünerek Wirofon uygulamasının bir önceki sürümünü yükledim ve ConfigServlet sayfasından gelen yanıtta aşağıdaki parametreyi farkettim. Uygulama bu parametreyi gördüğünde Wirofon uygulamasının yeni sürümünün çıktığına dair kullanıcıyı uyarmakta ve yeni sürümü indir butonuna basıldığında **latest_version_download_url** parametresinde yer alan adresten uygulamanın yeni sürümünü indirmeye çalışmaktaydı.

"latest_version" value="0.2.7">

Bende aynı şekilde sunucu ile uygulama arasına girerek bu parametreyi 0.2.8 (malum son sürüm 0.2.7 olunca güncelleme fonksiyonunu tetiklemek için sürümü 1 arttırdım) olarak değiştirmenin yanı sıra kendi web sayfamın adresinin yer aldığı latest_version_download_url parametresinide kullanıcıya gönderdiğimde otomatik güncelleme fonksiyonunu tetikletmeyi başarabildim.

Peki ya SSL ? Internet tarayıcılarında olduğu gibi MITM (ortadaki adam) saldırısının başarıya ulaşması için araya girildiğinde program bizi uyarmaz mı veya iletişimi kesmez mi ? Wirofon uygulaması SSL doğrulaması yapmadığı için ne yazık ki hayır.

Peki hepsi bu kadar mı ? İncelemek lazım.

```
key="sip_http_tunnel_type" value="https">
key="rtp_http_tunnel_type" value="https">
key="sip_http_tunnel_server" value="212.174.177.67|443">
key="rtp_http_tunnel_server" value="212.174.177.67|443">
```

Konfigürasyon parametrelerini dikkatlice inceleyecek olursanız SIP, RTP tünel sunucu adreslerinin ve haberleşme türünün bu parametrelerde yer aldığını görebilirsiniz. MITM (ortadaki adam) saldırısı gerçekleştiren art niyetli bir kişi https parametresini http ile değiştirir ve sunucu adreslerini kendi proxy sunucu adresi ile değiştirirse görüşmelerinizin şifresiz bir protokol üzerinden ve farklı bir sunucu üzerinden gerçekleşmesini sağlayabilir mi ?

Teorik olarak evet fakat pratik olarak denemediğim için net birşey söylemem mümkün değil buna rağmen dikkat edilmesi gereken diğer bir nokta olduğu için sizlerle paylaşmak istedim.

ISP seviyesi ve işletim sistemi seviyesinde gerçekleştirilen müdahaleler hariç MITM (ortadaki adam) ve evilgrade saldırılarının başarıya ulaşabilmesi için art niyetli kişinin sizinle aynı LAN/WLAN üzerinde olması gerektiği için bunun kritik bir güvenlik açığı olduğunu söylemem doğru olmaz fakat yinede ortak internet kullanımının (yurtlar, cafeler vs.) yaygın olduğu lokasyonlardan internete bağlanan Wirofon kullanıcılarının dikkatli olmasında fayda var.

Wirofon kullanıcılarına öneri olarak otomatik güncelleme mesajı ile karşılaşmaları durumunda programın indirildiği ip adresini kontrol etmelerini, Türk Telekom'a çözüm önerisi olarak ise Wirofon uygulamasında SSL doğrulamasını aktif hale getirmelerini ve otomatik güncelleme esnasında uygulamanın sunucudan gelen paketleri doğrulayabilmesi için Gtalk uygulamasında olduğu gibi dijital imza kullanmalarını önerebilirim.

Ve son olarak amacımın daha önceki tüm yazılarımda olduğu gibi bağcıyı dövmek olmadığını, her insan gibi üzümü yemeden önce kurtlu mu yoksa GDO'lu mu diye kontrol etmek olduğunu belirtmek isterim.

Konu ile ilgili olarak art niyetli bir kişi tarafından gerçekleştirilebilecek evilgrade saldırısını simüle eden kısa bir video hazırladım, herkese iyi seyirler dilerim.