MacGyver Olsaydı..

written by Mert SARICA | 1 Mart, 2013

80'lerde benim gibi çocuk olanların kahramanı çoğunlukla ya Michael Knight ya da MacGyver'dır. MacGyver, Kanada'da çekilmiş aksiyon-macera türünde bir Amerikan televizyon dizisiydi. Ajanımız Macgyver, silah kullanmayı sevmeyen, hemen hemen her bölümde fizik bilgisini kullanarak çevresinde bulduğu araç gereçlerden silah yaparak düşmanlarının elinden kolaylıkla kurtulabilmekteydi. Hatta bir bölümde MacGyver, etrafı gözetleyen bir kameranın hemen altında, kör noktada durup kameranın izlediği yolun fotoğrafını çekmiş, ardından bu resmi kameranın önüne koymuş ve kameranın çekilen bu fotoğrafı görüntü olarak güvenlik görevlilerine aktarmasını sağlayarak yakalanmadan koşar adımlarla oradan uzaklaşabilmiştir. Peki ya MacGyver günümüzde olsaydı ve geçmesi gereken bir kapının hemen arkasında kapıyı çeken ve kablosuz haberleşen bir IP kamera olsaydı ne yapardı ?

Geçtiğimiz aylarda satın aldığım Arduino Uno R3 cihazını gözetleme kamerasına çevirme girişimimin astarı yüzünden pahalıya (kablosuz ağ kalkanı, kamera vs.) geleceğini düşünerek IP kamera arayışı içine girdim ve çok geçmeden Türkiye'de Uranium markası altında satılan (Dünya'da WANSVIEW NCB-541W) SIP-10 modelini satın aldım. Cihazın kablosuz ağ desteklemesi, gece görüşünün olması, hareket algılama ve e-posta gönderme özelliğinin olması, fiyatı ve tabii ki uzaktan yönetilmeye imkan tanıyan Android uygulaması ile birlikte gelmesi satın alma kararı almamda etkili oldu.

Her zamanki gibi aldığım bir cihazı hacklemeye çalışmak, efendi efendi kullanmaktan çok daha cazip geldiği için geleneği bozmayarak kamerayı kurmadan önce kurulum CD'si ile birlikte gelen uygulamalara göz atmaya ve MacGyver olsaydı ne yapardı? sorusuna yanıt aramaya karar verdim.

Ağda bulunan kamerayı tespit etmek ve yeni ip adresi tanımlamak için kullanılan BSearch_en.exe dosyasını Immunity Debugger aracı ile biraz inceledikten sonra kamerayı kurup çalıştırdım ve ağ seviyesinde uygulamanın nasıl çalıştığını kısaca inceledim.

IP kamera varsayılan olarak 192.168.0.178 ip adresi ile birlikte gelmekte ve BSearch uygulaması tarafından BROADCAST adrese gönderilen UDP paketlerine (SEARCH ve UPDATE) yanıt vererek kullanıcının kamerayı tespit etmesine (SEARCH) ve ayarları değiştirmesine (UPDATE) imkan tanımaktadır.

Tabii ayarları değiştirebilmek için (UPDATE) öncelikle kullanıcının ip kamerasının yönetim kullanıcı adı ve şifresini doğru girmesi gerekmektedir aksi halde tanımlarda herhangi bir değişiklik yapamamaktadır.

Kameraya giden ve gelen veriyi dikkatlice incelediğim de MO_I parametresi dikkatimi çekti. MO_I parametresinden sonra gelen bayt'ın SEARCH paketinde 00, UPDATE paketinde ise 02 olduğunu farkettim.

Cihaz üreticileri çoğunlukla hata ayıklamak (debug) ve/veya geliştirme amacıyla cihazlara arka kapı bırakmayı sevdiklerinden ötürü bu bayt üzerinde Fuzzing yapmaya karar verdim ve bunun için Python ile sip-10_fuzzer.py adında bir program hazırladım. Programı çalıştırdıktan sonra Fuzz edilen baytın 78 olduğu durumda, cihazın yeniden başladığını farkettim. Ardından cihaza SEARCH paketi gönderdiğim de cihazın MAC adresinin değişmiş olduğunu farkettim.

Sonuç olarak yaptığım kısa araştırma sonucunda SIP-10 IP kamerasında keşfettiğim bu güvenlik zafiyeti ile cihazı yetkisi olmayan ve ağda bulunan herhangi bir kişinin uzaktan yeniden başlatabildiğini ve MAC adresini değiştirebildiğini tespit etmiş oldum. Gelelim MacGyver olsaydı ne yapardı sorusunun yanıtına. Muhtemelen kahramanımız kablosuz ağa dahil olur ve göndereceği tek bir paket ile kamerayı geçici süreliğine devre dışı bırakarak kameraya yakalanmadan yoluna emin adımlarla devam ederdi :)

MacGyver'ın yerinde herhangi bir hırsızın olmaması dileğiyle herkese güvenli günler dilerim.