

# MacGyver Olsaydı...

written by Mert SARICA | 1 March 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.

```
Frame 26 (69 bytes on wire, 69 bytes captured)
Ethernet II, Src: vmware_75:0d:93 (00:0c:29:75:0d:93), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.1.40 (192.168.1.40), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: 62010 (62010), Dst Port: ndmp (10000)
Data (27 bytes)
Data: 4d4f5f490000000000000000000000040000000000000000...
```

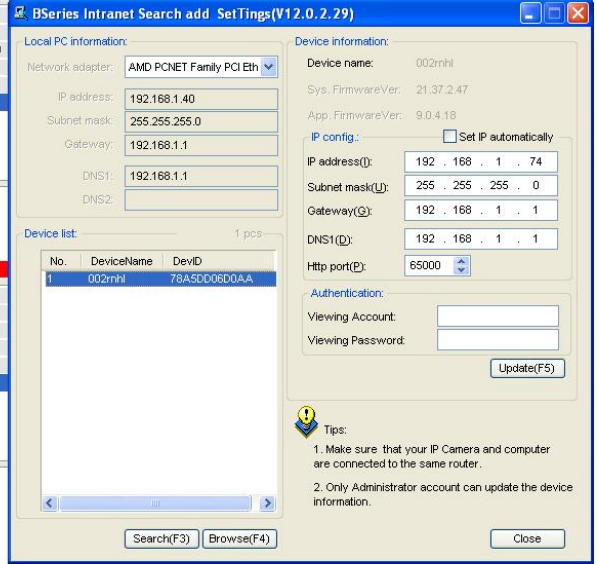
### SEARCH - GİDEN PAKET

```
0000 ff ff ff ff ff ff 00 0c 29 75 0d 93 08 00 45 00 ..... )u....E.
0010 00 37 ad 20 00 00 80 11 cb c5 c0 a8 01 28 ff ff .7. .... (.
0020 ff ff f2 3a 27 10 00 23 76 f0 4d 4f 5f 49 00 00 .....# v..MO..I.
0030 00 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 .....
0040 00 00 00 00 00
```

```
Frame 27 (130 bytes on wire, 130 bytes captured)
Ethernet II, Src: 48:02:2a:4e:fe:37 (48:02:2a:4e:fe:37), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.1.74 (192.168.1.74), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: ndmp (10000), Dst Port: 62010 (62010)
Data (88 bytes)
Data: 4d4f5f49010000000000000000000410000004100000037...
```

### SEARCH - GELEN PAKET

```
0000 ff ff ff ff ff ff 48 02 2a 4e fe 37 08 00 45 00 .....H. *N.7..E.
0010 00 74 0f 00 40 00 40 11 78 87 c0 a8 01 4a ff ff .t..@.@. x....J..
0020 ff ff 27 10 f2 3a 00 60 48 f2 4d 4f 5f 49 01 00 ..... H..MO...
0030 00 00 00 00 00 00 00 00 00 41 00 00 00 41 00 00 .....A..A..
0040 00 37 38 41 35 44 44 30 36 44 30 41 41 00 30 30 .....78A5DD0 6D0AA..00
0050 32 72 6e 68 6c 00 00 00 00 00 00 00 00 00 00 00 .....2rnhl...
0060 00 00 00 c0 a8 01 4a ff ff ff c0 a8 01 01 c0 .....J.
0070 88 01 01 00 00 00 00 15 25 02 2f 09 00 04 12 fd .....%./...
0080 88 00
```



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

```
Frame 82 (129 bytes on wire, 129 bytes captured)
Ethernet II, Src: vmware_75:0d:93 (00:0c:29:75:0d:93), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.1.40 (192.168.1.40), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: 62010 (62010), Dst Port: ndmp (10000)
Data (87 bytes)
Data: 4d4f5f4902000000000000000000040000000000000000...
```

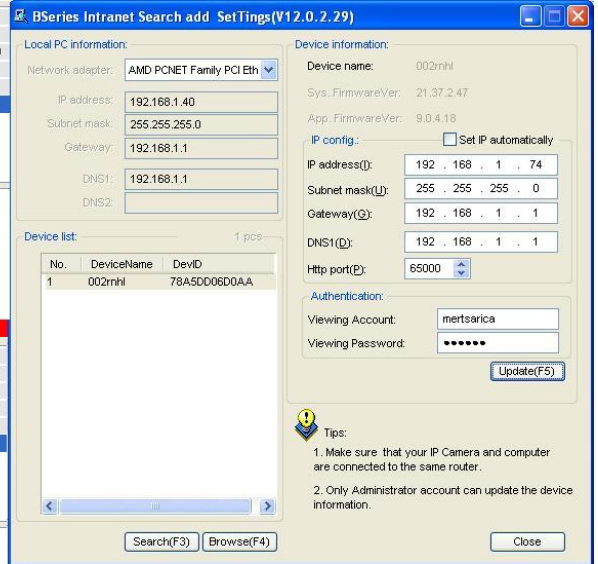
### UPDATE - GİDEN PAKET

```
0000 ff ff ff ff ff ff 00 0c 29 75 0d 93 08 00 45 00 ..... )u....E.
0010 00 73 af 0e 00 00 80 11 c9 9b c0 a8 01 28 ff ff .5..@.@. x....J..
0020 ff ff f2 3a 27 10 00 5f 12 fa 4d 4f 5f 49 02 00 .....78A5DD06D0AA...
0030 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 .....
0040 00 00 00 00 01 37 38 41 35 44 44 30 36 44 30 41 .....78A 5DD06D0A
0050 41 00 6d 65 72 74 73 61 72 69 63 61 00 00 00 31 .....A.mertsarica...1
0060 32 33 34 35 36 00 00 00 00 00 00 00 c0 a8 01 4a .....23456...J
0070 ff ff ff c0 a8 01 01 c0 a8 01 01 fd e8 00 00 .....
0080 00
```

```
Frame 83 (67 bytes on wire, 67 bytes captured)
Ethernet II, Src: 48:02:2a:4e:fe:37 (48:02:2a:4e:fe:37), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.1.74 (192.168.1.74), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: ndmp (10000), Dst Port: 62010 (62010)
Data (25 bytes)
Data: 4d4f5f4903000000000000000000020000000200000001...
```

### UPDATE - GELEN PAKET

```
0000 ff ff ff ff ff ff 48 02 2a 4e fe 37 08 00 45 00 .....H. *N.7..E.
0010 00 35 00 00 40 00 40 11 78 c6 c0 a8 01 4a ff ff .5..@.@. x....J..
0020 ff ff 27 10 f2 3a 00 21 74 d1 4d 4f 5f 49 03 00 .....! t..MO..I.
0030 00 00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 .....
0040 00 01 00
```



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 sevdiğlerinden 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.



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