Mavi Tehlike

written by Mert SARICA | 2 May 2017

Logosunu, Danimarka'nın ilk kralı olan 10. Yüzyıl Viking savaşçısı Harald "Mavidiş" Gormsson'un baş harflerinin runik alfabesindeki karşılığından (ve) alan Bluetooth kablosuz ağ teknolojisi, cep telefonları ile önce cebimize, sonrasında Bluetooth Low Energy (BLE) olarak IoTler ile hayatımıza gireli epey oldu.

2000'li yılların ortalarına doğru, BlueSnarfing yöntemi ile art niyetli kişilerin Nokia ve Ericsson marka cep telefonlarında bulunan zafiyet sayesinde Bluetooth üzerinden bilgimiz ve iznimiz olmadan mesajlarımıza, adres defterimizi ulaşabildiğini gördük. Ardından Bluejacking yöntemi ile hedef telefona vCard formatında istenmeyen mesajlar gönderilebildiğini, Bluebugging yöntemi ile de bilgisayarımızın, cep telefonumuzun art niyetli kişilerce kontrol edilebildiğini öğrendik. Commwarrior zararlı yazılımı ile Bluetooth'un atak vektörü olarak nasıl kullanılabileceğini tecrübe etmiş olduk. Tabii ortaya çıkan tüm bu zafiyetlerin, kötüye kullanımların temelinde Bluetooth'un ta kendisinin değil aksine üreticiler tarafından hatalı kullanılmasının (implementation) olduğunu unutmamamız gerekmektedir.

Geçmişten günümüze dönecek olursak, artık modern ve güncel akıllı cihazlarda eskiden olduğu gibi Bluetooth, keşfedilebilir kipte çalışmıyor. Örneğin Android 6.0.1 işletim sisteminde (ve iOS'ta da benzer şekilde), diğer cihazların sizin cihazınıza Bluetooth üzerinden bağlanabilmesi için Ayarlar'dan Bluetooth menüsüne girmeniz gerekiyor. Durum böyle olunca güvenlik ve mahremiyet adına çok endişe etmenize gerek kalmıyor. Güncel olmayan sistemlerde ise Bluetooth'u devre dışı bırakarak potansiyel tehlikelerden kaçınabiliyoruz.

Peki ya evimizde kullandığımız akıllı, akılsız internete bağlanan nesneler (IoT) ? Bluetooth üzerine biraz düşünürken aslında evimizde kullandığımız nesnelerin, akıllı cihazların hırsızlara, art niyetli kişilere davetiye çıkardığını gördüm. Örneğin evimde, üzerinde Bluetooth desteği bulunan ve her daim Bluetooth servisi açık (hata #1) olan akıllı bir televizyonum var. Televizyonumu ne zaman açsam Bluetooth üzerinden haberleşmeye açık konumda bekliyor ve bağlantı kurulana dek adını ([TV]Samsung LED48 – hata #2) etrafa yayınlıyor. (broadcast)

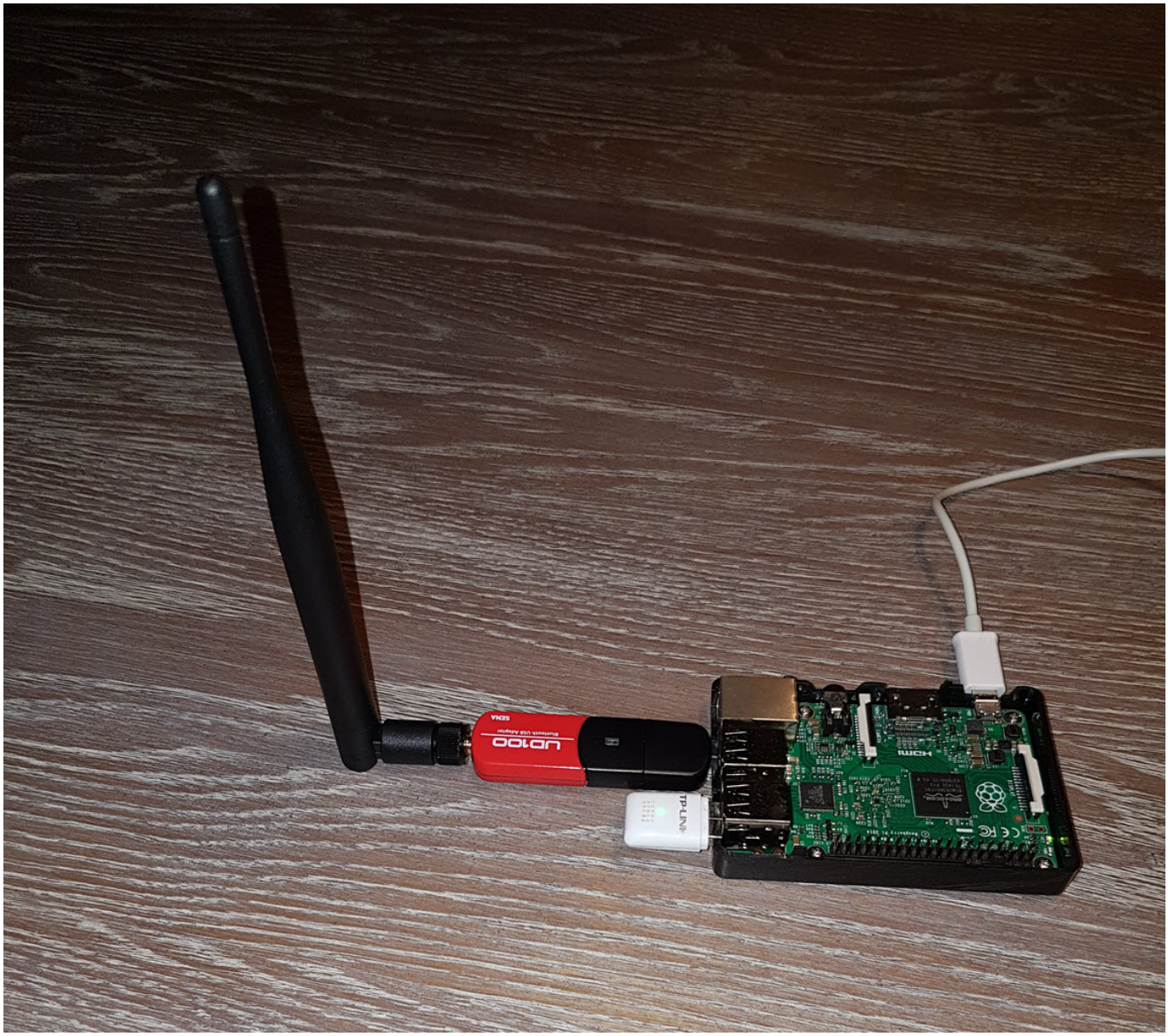
Genellikle hırsızların hacking döngüsünde de olduğu gibi bir eve girmeden

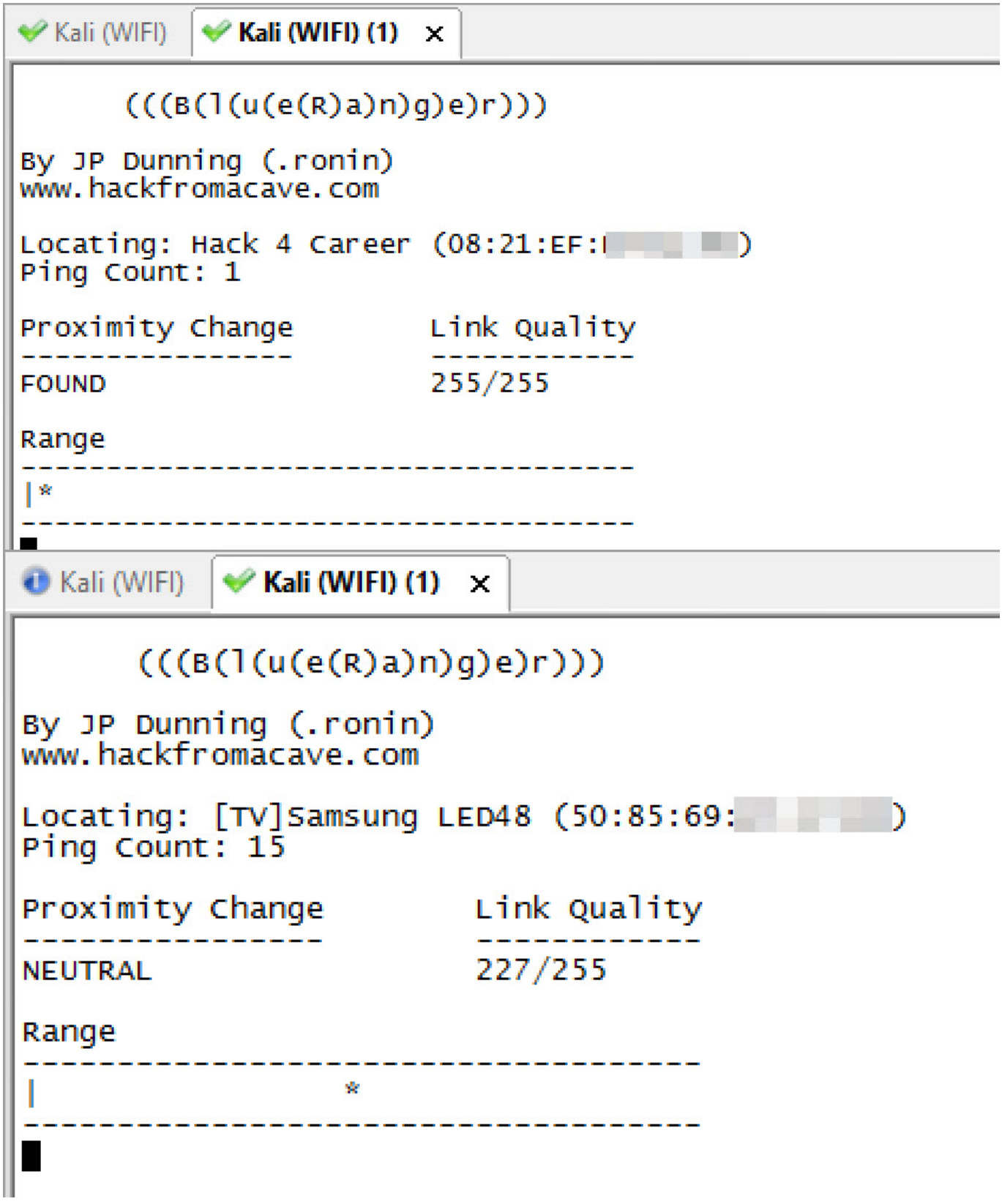
önce aktif ve pasif keşif çalışması yaptıklarını biliyoruz. Gece ise evin ışıkları yanıyor mu ? Perdeler kapalı mı ? Zili çalınca kim o diye soran var mı ? gibi gibi. Peki günümüzde Bluetooth teknolojisi hırsızlar tarafından nasıl kötüye kullanılabilir ?

Kısa mesafe teknolojisi olarak bilinen Bluetooth teknolojisinin aksine, sınıfına (class) göre 100 metre mesafeye kadar haberleşme sağlayabildiğini görebiliriz. Parani UD-100 gibi bir aygıt ve uygun anten ile bu mesafenin 600 metre ila 1 KM'ye kadar genişletilebildiğini düşündüğümüz de, art niyetli kişilerin uzak mesafeden bluetooth kullanan aygıtlarımızı izleme hatta müdahale etme imkanı olduğunu az çok tahmin edebiliriz.

Özellikle işaret gücü göstergesi (RSSI) bilgisinden faydalanarak etrafınızda bulunan bir Bluetooth aygıtın size ne kadar yakın olduğunu kestirebilirsiniz. Kali Linux ile birlikte gelen ve l2cap'ten faydalan BlueRanger aracı da size bu konuda yardımcı olabiliyor.

Bu bilgiler ışığında üzerinde Kali Linux çalışan ve Parani UD-100 USB adaptörü takılı olan bir Raspberry Pi 3 ile bazı araçlardan faydalanarak ufak testler yapmaya karar verdim. İlk olarak Blueranger aracına Parani UD-100 USB adaptörünün oldukça yakınında tutarak, bluetooth ekranı açık olan Android 6.0.1 çalışan cep telefonumun MAC adresini verdim. Ardından salonun diğer ucunda bulunan akıllı televizyonumun MAC adresini verdiğim de ortaya çıkan sonuçlar beni tatmin etti.


UD100
Bluetooth USB Adapter
SEKA
HDMI

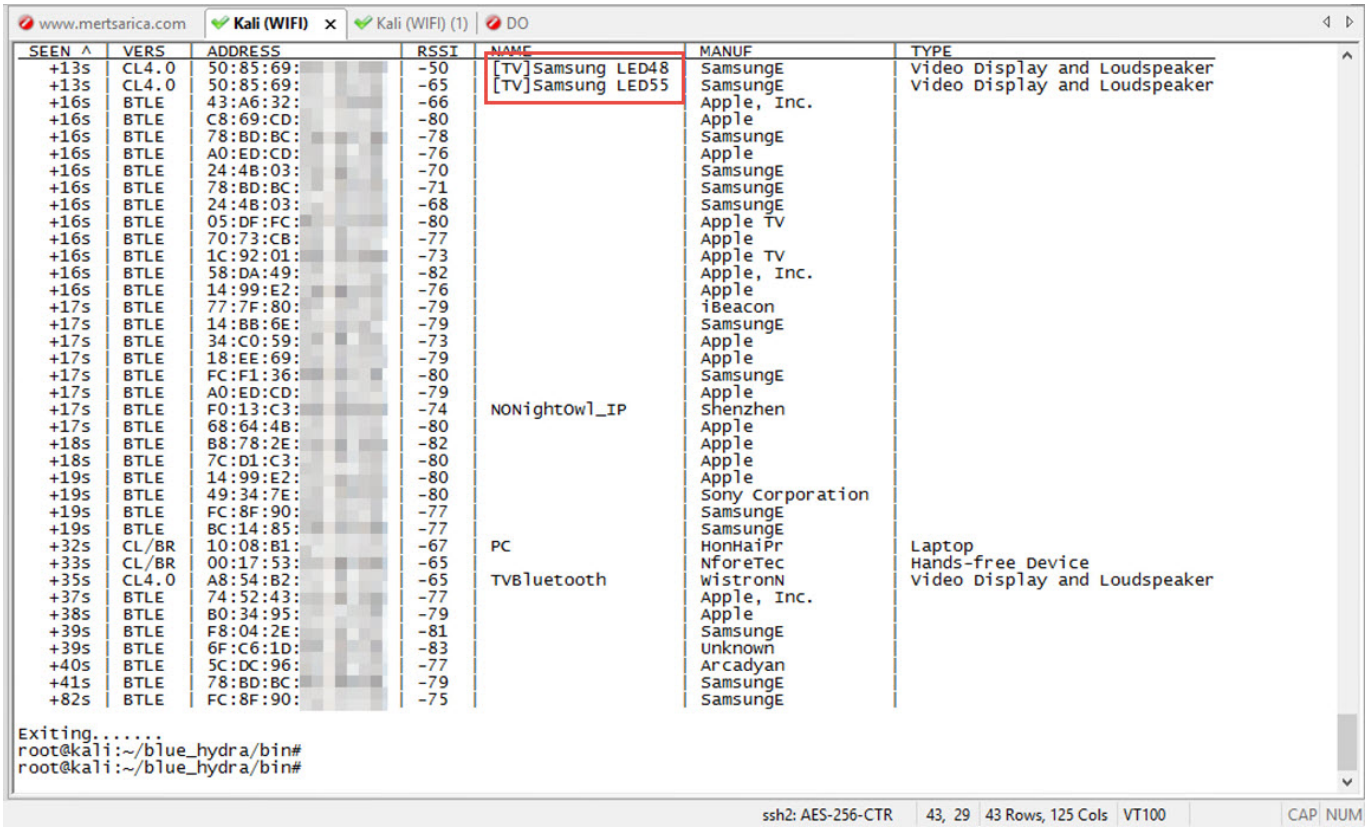


Tabii işi biraz daha ileriye götürüp etraftaki Bluetooth cihazlardan, aygıtlardan daha detaylı bilgi almaya karar verdim ve bu defa Blue Hydra aracı ile ufak bir test gerçekleştirdim.

Blue Hydra aracı sızma testi cihazları ile adını duyurmuş Pwnie Express ekibi tarafından geliştirilmekte olan, tespit etiği Bluetooth aygıtları, cihazları ve topladığı bilgileri arka planda veri tabanında saklayabilen oldukça

faydalı bir araçtır.

Raspberry Pi'yi evde camın kenarına yaklaştırdığımda, Blue Hydra sayesinde etrafımda çok sayıda Bluetooth cihaz olduğunu üretici, tür, sürüm, işaret gücü göstergesi (RSSI) bazında görebildim. Hatta RSSI bilgisi sayesinde ya üst ya da alt kattaki komşumun 55 ekran Samsung televizyonu olduğunu tespit edebildim.



Bu bilgileri ben toplayabiliyorsam herkes toplayabilirden yola çıkacak olursak, art niyetli kişilerin, teknolojiden faydalanabilen hırsızların bu yöntem ile kendileri için değerli olabilecek bilgileri toplayabileceğini öğrenmiş oldum.

Güvenliğiniz, mahremiyetiniz adına cep telefonundan, evinizde kullanmış olduğunuz nesnelerin internetine (IoT) kadar tüm cihazlarınızda, sistemlerinizde kullanmadığınız sürece Bluetooth servisini kapalı tutmanızı ve çevrenizdekilere de bunu tavsiye etmenizi öneririm.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.