Casus Fare

written by Mert SARICA | 1 December 2017
If you are looking for an English version of this article, please visit here.

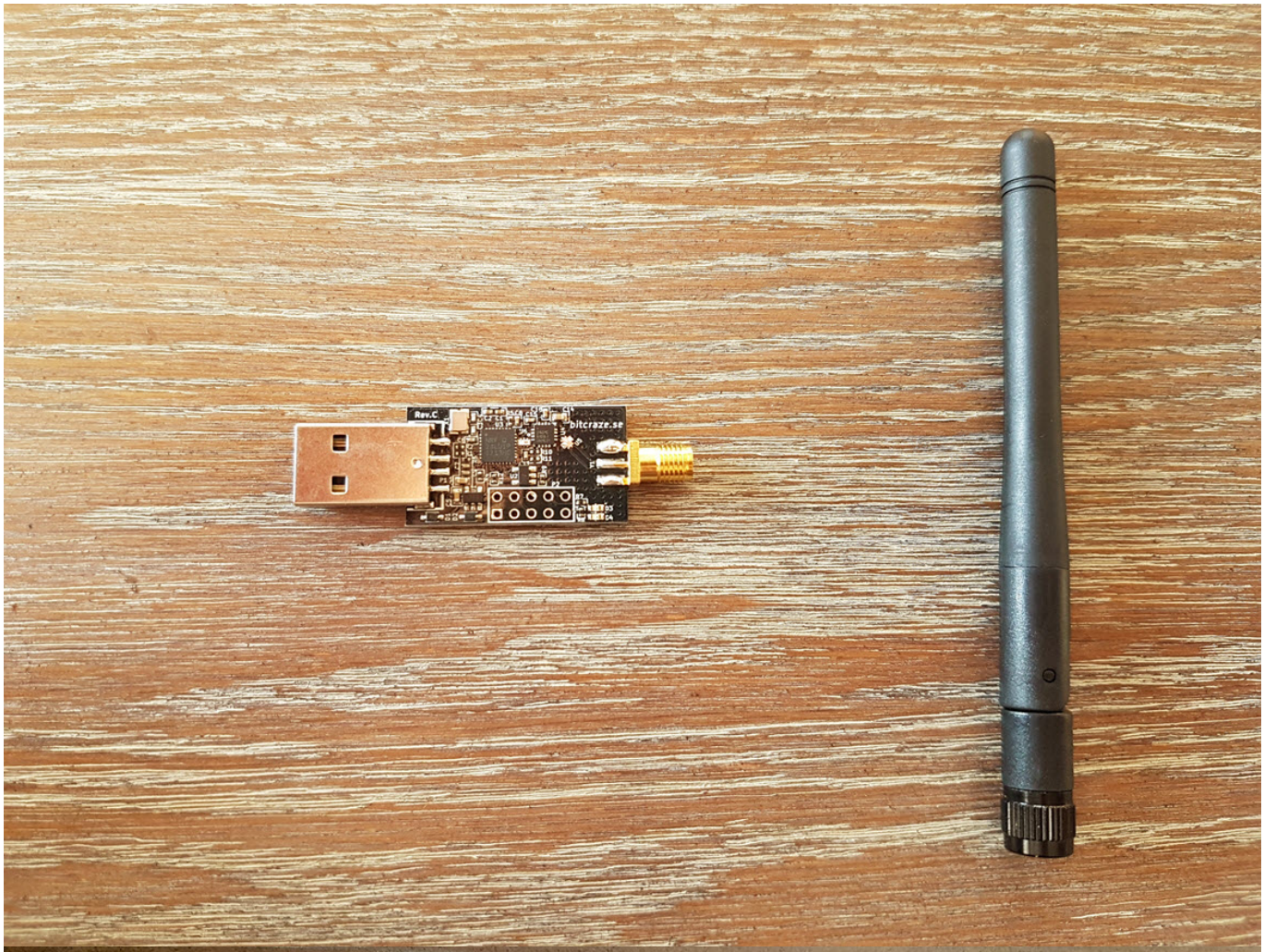
2015 yılında elektronik ürünler satan bir mağazada kampanyada olan bir ürün seti dikkatimi çekmişti. Kaspersky Internet Security güvenlik yazılımını satın aldığınız taktirde Microsoft'un Sculpt Mobile model kablosuz faresi hediye olarak geliyordu. Yeni bir fareye ihtiyacım olduğu için o zamanlar hiç düşünmeden satın aldığım ve yıllardır severek kullandığım bu kablosuz farenin, sahip olduğu zafiyet nedeniyle arkamdan işler çevirebilecek bir casusa dönüşebileceği hiç aklıma gelmemişti. :)

Bluetooth olmayan kablosuz klavye ve farelerin RF haberleşmesi üzerine yapılan araştırmalara kısaca bakacak olursak, 2007 yılında Max Moser tarafından 27 MHz bandında haberleşen kablosuz klavyelerin (Microsoft ve Logitech) uzaktan rahatlıkla dinlenebileceği, yaptığı bir araştırma sonucunda ortaya çıktı ve güvenlik dünyasında oldukça ses getirdi. 2009 yılında ise Max Moser ve Thorsten Schroeder, kablosuz klavyeleri dinlemek amacıyla geliştirdikleri ve KeyKeriki adını verdikleri aygıtı duyurdular. 2010 yılında ise bu defa 2.4 GHz bandından haberleşen ve Nordic Semiconductor NRF24XXX çipine sahip klavyeleri de dinleyebilen KeyKeriki v2.0'ı duyurdular. 2011 yılında Travis Goodspeed, ~5TL değerinde olan nRF24L01+ çipini promiscuous kipte çalıştırarak 2.4 GHZ bandında NRF24XXX çipler tarafından gönderilen paketlerin basit bir şekilde izlenebileceğini (sniff) gösterdi. 2015 yılında Samy Kamkar, Arduino tabanlı KeySweeper aygıtı ile Microsoft klavyelerden tuş bilgilerinin anlık olarak pratik bir şekilde nasıl çalınabileceğini tüm dünyaya gösterdi.

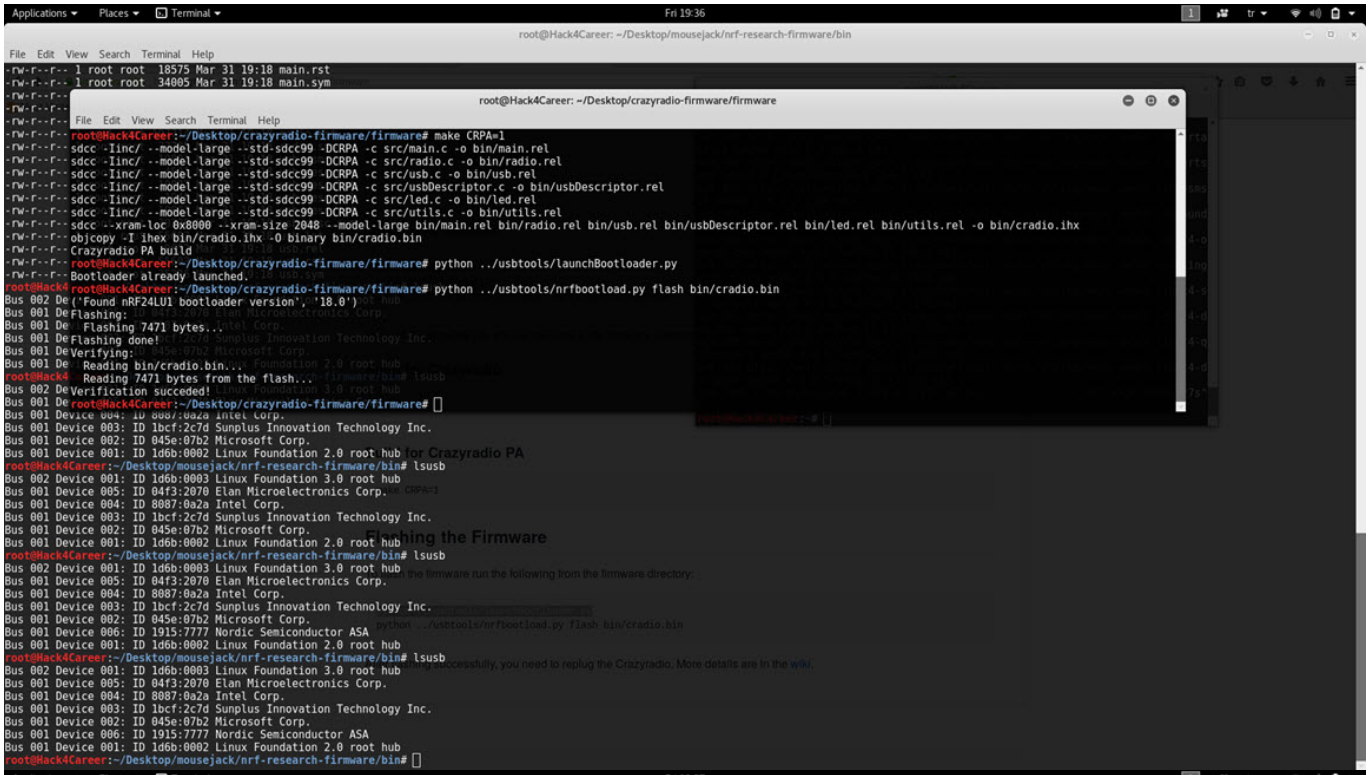
Yıllar içinde yapılan bu araştırmalar ve çalışmalar sayesinde bluetooth olmayan kablosuz klavyeler (2.4 GHz ISM) ile bilgisayarlar arasındaki RF haberleşme, üreticiler tarafından (istisnalar hariç) güçlü algoritmalarla şifrelenerek art niyetli kişiler tarafından tuş bilgilerinin izlenmesinin önüne geçildi. Üreticiler kablosuz klavyeleri güvenli hale getirmek için yoğun çaba sarfederken, kablosuz fareler arka planda kaldı. Ne de olsa bir farenin hareketlerinin ve basılan buton bilgilerinin (sağ, sol, orta) şifresiz çalınması art niyetli kişilerin ne işine yarayabilir ? İşin aslının pek de öyle olmadığını 2015 yılında Bastille firmasının yapmış olduğu ve MouseJack adını verdiği araştırma ve çok sayıda üreticinin etkilendiği yöntem

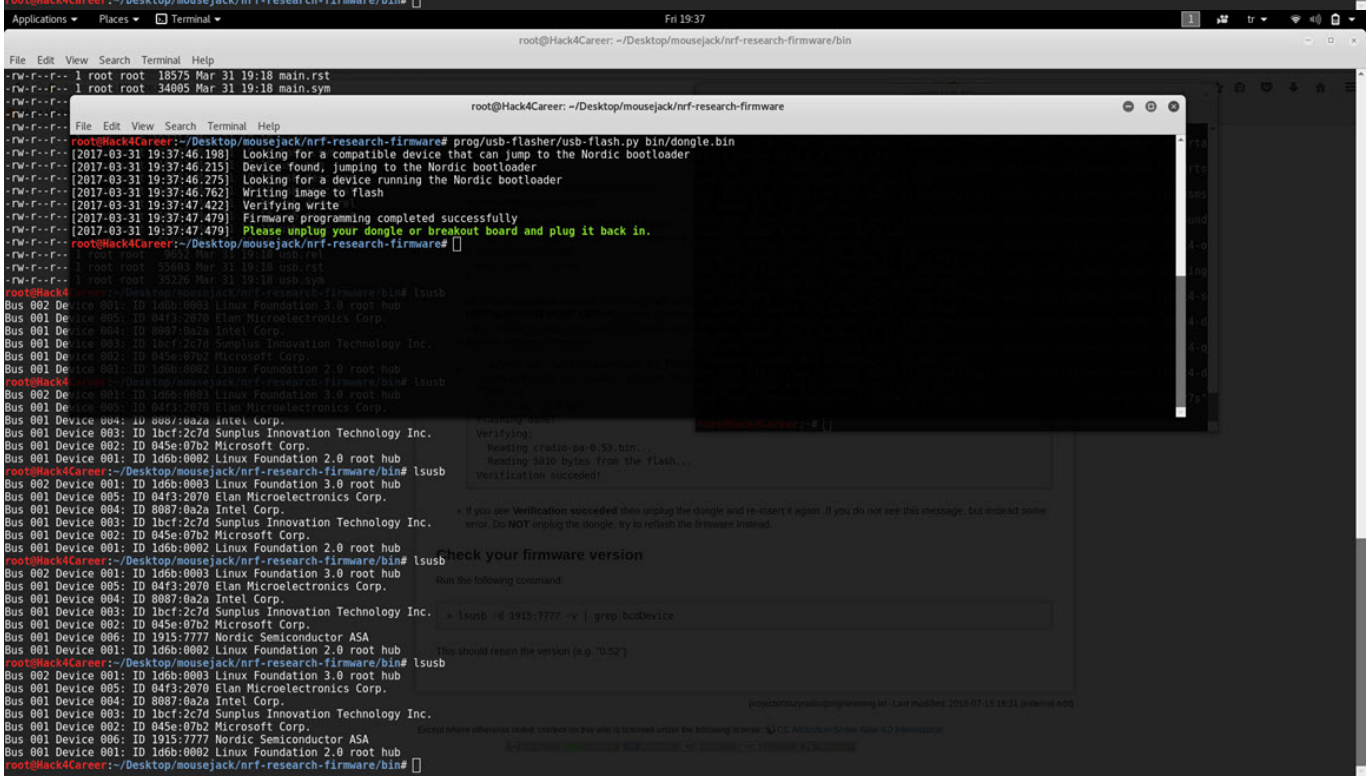
ile ortaya koymuş (video) oldu. MouseJack yöntemi ile fare alıcısı olarak bilgisayara takılan USB alıcıya fare hareket ve basılan butonların bilgilerinin yerine kablosuz olarak Bad,Bad USB blog yazımda olduğu gibi Ducky Script formatında klavye tuş basma bilgileri (keystroke) gönderilmektedir. Bu sayede benim gibi dizüstü bilgisayar kullandığınız için kablosuz klavye kullanmasanız da, kablosuz fare kullandığınız için bilgisayarınızın başından kısa süreliğine kalktığınızda, art niyetli bir kişi kablosuz olarak bilgisayarınıza bağlı olan USB alıcıya kablosuz fareden gönderiliyormuş gibi istediği tuş basma bilgilerini gönderebilmektedir!

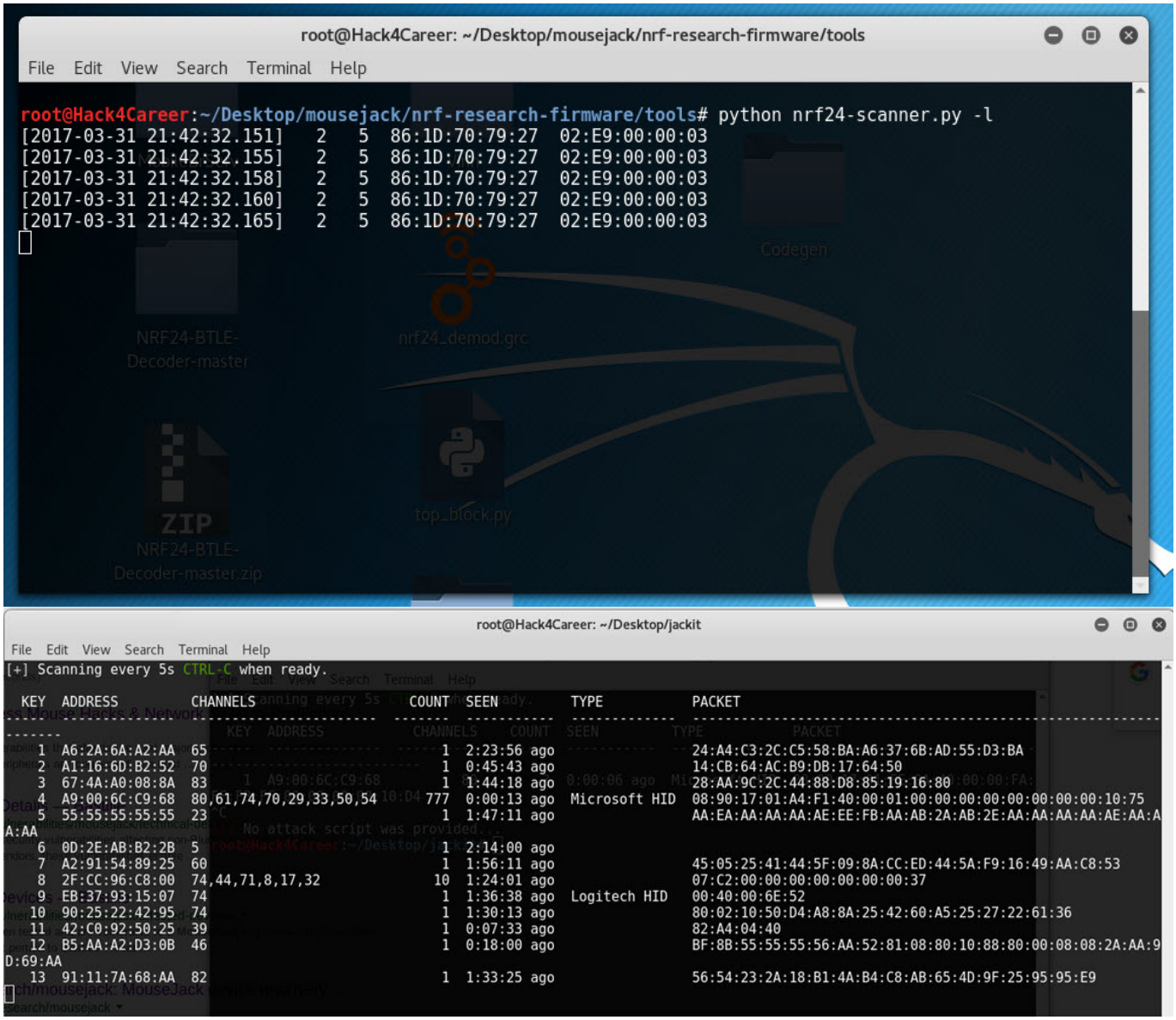
Kablosuz Microsoft fare kullanan biri olarak, MouseJack yönteminin farem üzerinde etkili olup olmadığını anlamak için hemen işe koyuldum ve Bastille'nin MouseJack GitHub sayfasında belirtildiği üzere CrazyRadio PA USB aygıtını satın almaya karar verdim. nrf-research-firmware donanım yazılımını derleyip, CrazyRadio PA'ya (bin/dongle.bin) yükledikten sonra Bastille'nin GitHub sayfasında yer alan araçların etraftaki nRF24L01+ aygıtları tespit etmeye ve paketleri izlemeye imkan tanıdığını gördüm. Bastille, klavye tuş basma bilgilerini gönderebilen aracını sadece üreticilerle paylaştığı için GitHub'da ufak bir araştırma yapmaya karar verdim ve çok geçmeden klavye tuş basma bilgilerini de göndermeye imkan tanıyan jackit aracı ile karşılaştım.


Rev.C
bitcraze.se

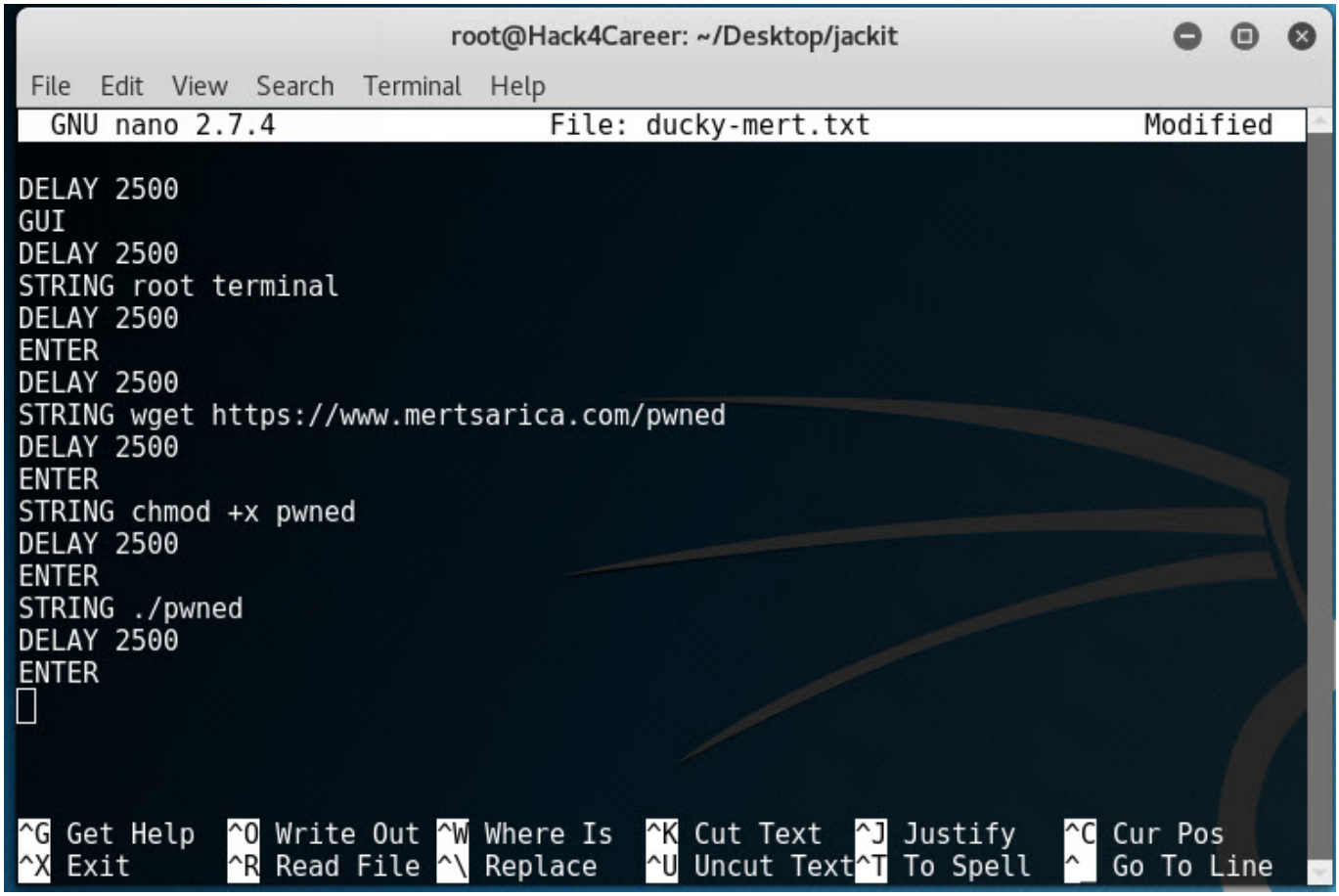



Applications Places Terminal Fri 19:36
root@Hack4Career: ~/Desktop/mousejack/nrf-research-firmware/bin
File Edit View Search Terminal Help
root@Hack4Career: ~/Desktop/crazyradio-firmware/firmware
root@Hack4Career:~/Desktop/crazyradio-firmware/firmware# make CRPA=1
root@Hack4Career:~/Desktop/crazyradio-firmware/firmware# python ../usbtools/launchBootloader.py
Bootloader already launched.
root@Hack4Career:~/Desktop/crazyradio-firmware/firmware# python ../usbtools/nrfbootload.py flash bin/cradio.bin
("Found nRF24LU1 bootloader version", '18.0')
Flashing:
Flashing 7471 bytes...
Flashing done!
Verifying:
Reading bin/cradio.bin...
Reading 7471 bytes from the flash...
Verification succeded!
root@Hack4Career:~/Desktop/crazyradio-firmware/firmware#
Bus 001 Device 004: ID 8087:0a2a Intel Corp.
Bus 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.
Bus 001 Device 002: ID 045e:07b2 Microsoft Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin# lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 005: ID 04f3:2070 Elan Microelectronics Corp.
Bus 001 Device 004: ID 8087:0a2a Intel Corp.
Bus 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.
Bus 001 Device 002: ID 045e:07b2 Microsoft Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin# lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 005: ID 04f3:2070 Elan Microelectronics Corp.
Bus 001 Device 004: ID 8087:0a2a Intel Corp.
Bus 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.
Bus 001 Device 002: ID 045e:07b2 Microsoft Corp.
Bus 001 Device 006: ID 1915:7777 Nordic Semiconductor ASA
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin# lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 005: ID 04f3:2070 Elan Microelectronics Corp.
Bus 001 Device 004: ID 8087:0a2a Intel Corp.
Bus 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.
Bus 001 Device 002: ID 045e:07b2 Microsoft Corp.
Bus 001 Device 006: ID 1915:7777 Nordic Semiconductor ASA
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin#


Applications Places Terminal Fri 19:37
root@Hack4Career: ~/Desktop/mousejack/nrf-research-firmware/bin
File Edit View Search Terminal Help
root@Hack4Career: ~/Desktop/mousejack/nrf-research-firmware
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware# prog/usb-flasher/usb-flash.py bin/dongle.bin
[2017-03-31 19:37:46.198] Looking for a compatible device that can jump to the Nordic bootloader
[2017-03-31 19:37:46.215] Device found, jumping to the Nordic bootloader
[2017-03-31 19:37:46.275] Looking for a device running the Nordic bootloader
[2017-03-31 19:37:46.762] Writing image to flash
[2017-03-31 19:37:47.422] Verifying write
[2017-03-31 19:37:47.479] Firmware programming completed successfully
[2017-03-31 19:37:47.479] Please unplug your dongle or breakout board and plug it back in.
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware#
Bus 001 Device 004: ID 8087:0a2a Intel Corp.
Bus 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.
Bus 001 Device 002: ID 045e:07b2 Microsoft Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin# lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 005: ID 04f3:2070 Elan Microelectronics Corp.
Bus 001 Device 004: ID 8087:0a2a Intel Corp.
Bus 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.
Bus 001 Device 002: ID 045e:07b2 Microsoft Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin# lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 005: ID 04f3:2070 Elan Microelectronics Corp.
Bus 001 Device 004: ID 8087:0a2a Intel Corp.
Bus 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.
Bus 001 Device 002: ID 045e:07b2 Microsoft Corp.
Bus 001 Device 006: ID 1915:7777 Nordic Semiconductor ASA
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin# lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 005: ID 04f3:2070 Elan Microelectronics Corp.
Bus 001 Device 004: ID 8087:0a2a Intel Corp.
Bus 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.
Bus 001 Device 002: ID 045e:07b2 Microsoft Corp.
Bus 001 Device 006: ID 1915:7777 Nordic Semiconductor ASA
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
root@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin#



Jackit aracını Kali'ye kurduktan hemen sonra Ducky Script formatında hazırladığım klavye tuş bilgilerini, Crazyradio PA ile göndermeye başladım. Kısa bir süre sonra Kali'de root terminal açıldı, wget ile https://www.mertsarica.com adresinden pwned dosyası indirildi ve çalıştırıldı.



Yapmış olduğum bu çalışma sonrasında sahip olduğum Microsoft marka kablosuz faremi üzülerek çöpe atıp, daha güvenli bir kablosuz fare almak için elektronik ürünler satan bir mağazanın yolunu tuttum. Fiziksel güvenliğim ve güvenlik farkındalığı için yapmış olduğum bu çalışmanın, kablosuz klavye ve fare kullananlar adına faydalı olmasını temenni eder, bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.