FORTINET

Medical Malware on Android

a.k.a Android malware affecting medical apps

Axelle Apvrille

No Hat, November 28, 2020

Hello! Who am I?

Axelle Apvrille

Principal Security Researcher at **Fortinet**, @cryptax

Mobile malware, IoT, Ph0wn CTF

Lots of Medical Apps on Android



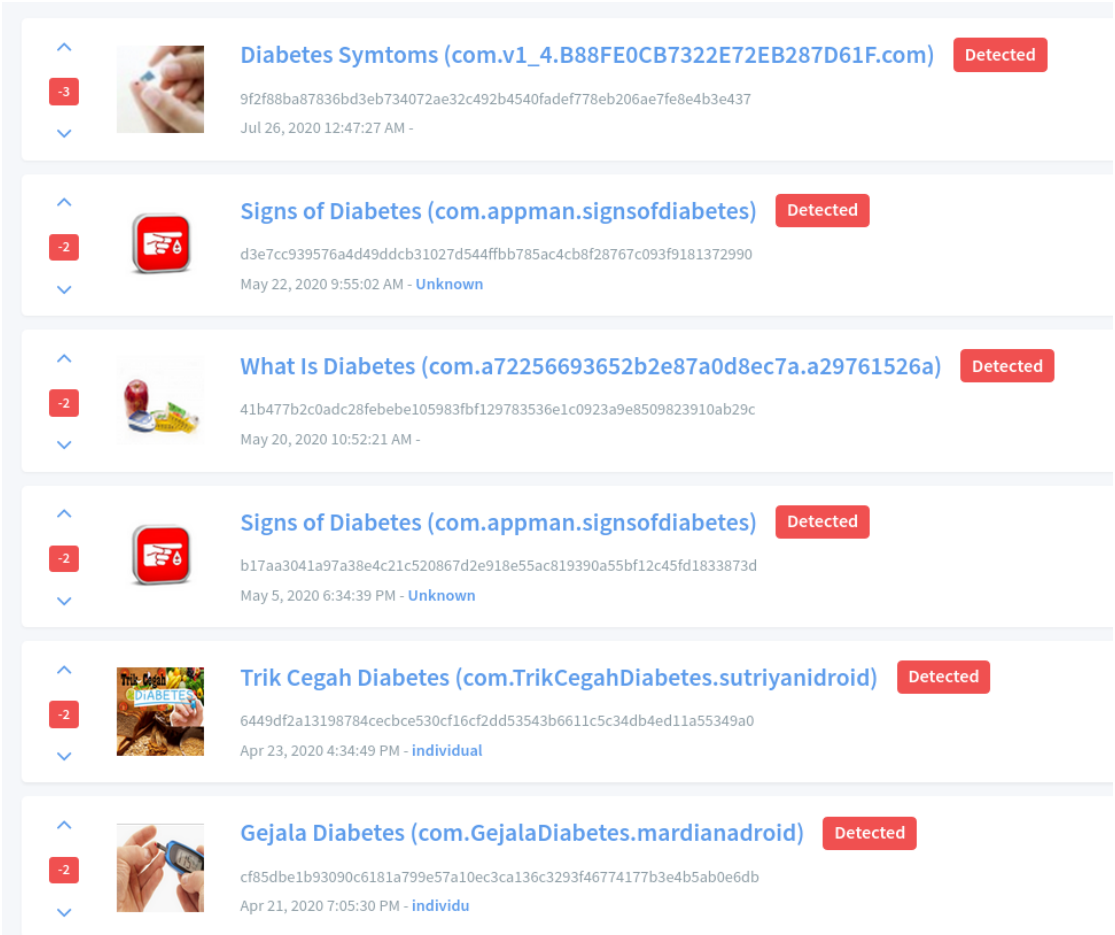




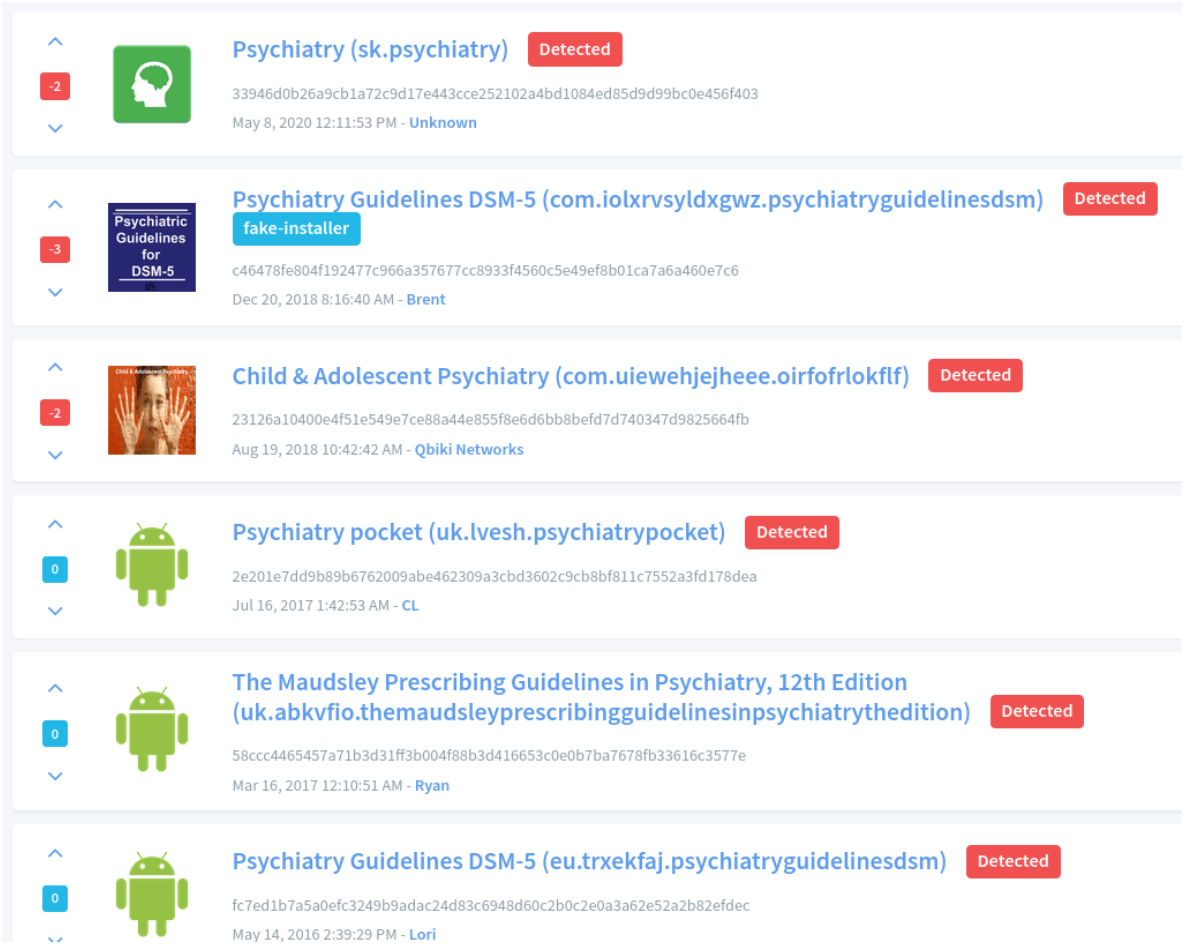




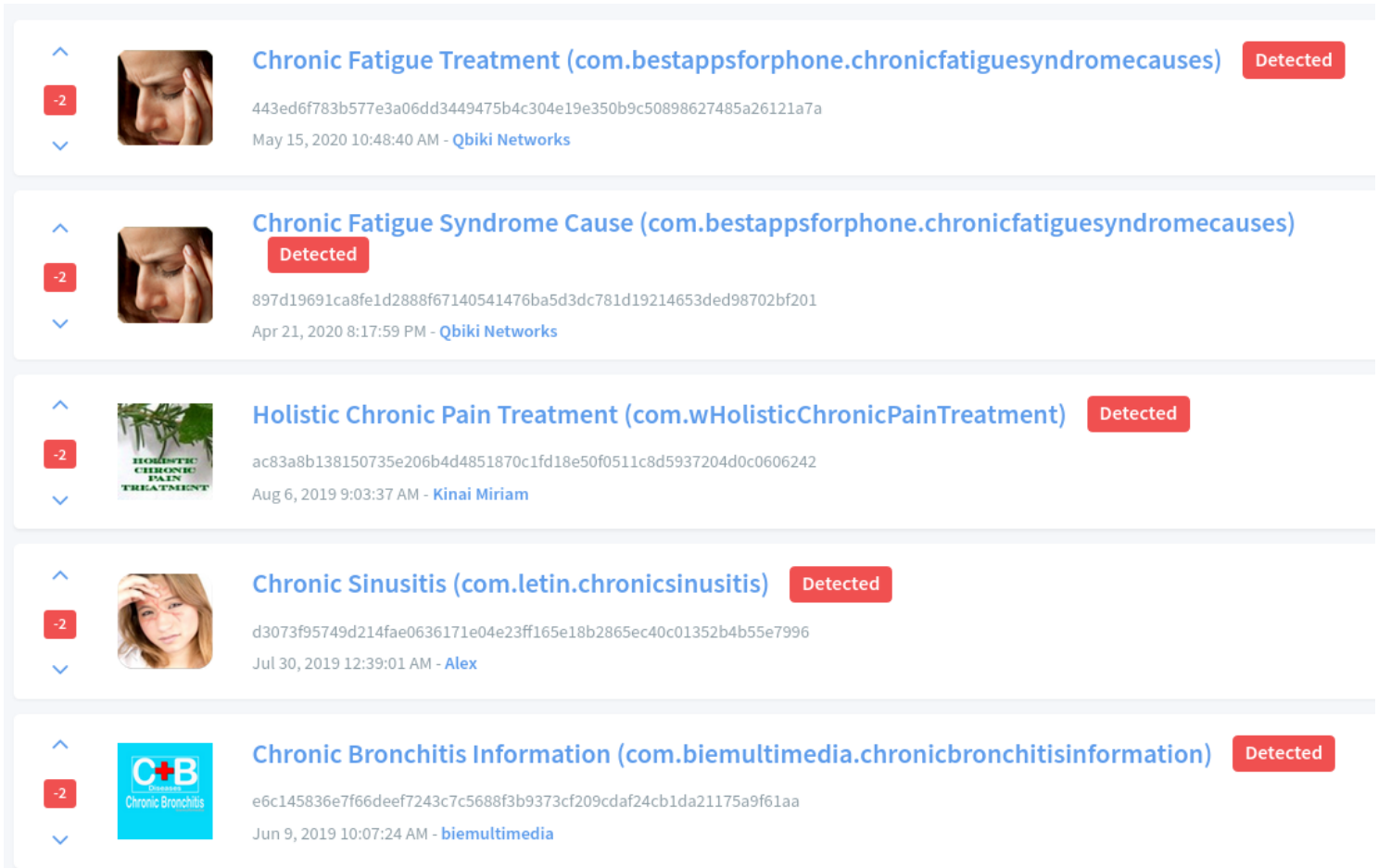
Malware in medical apps, fake apps etc



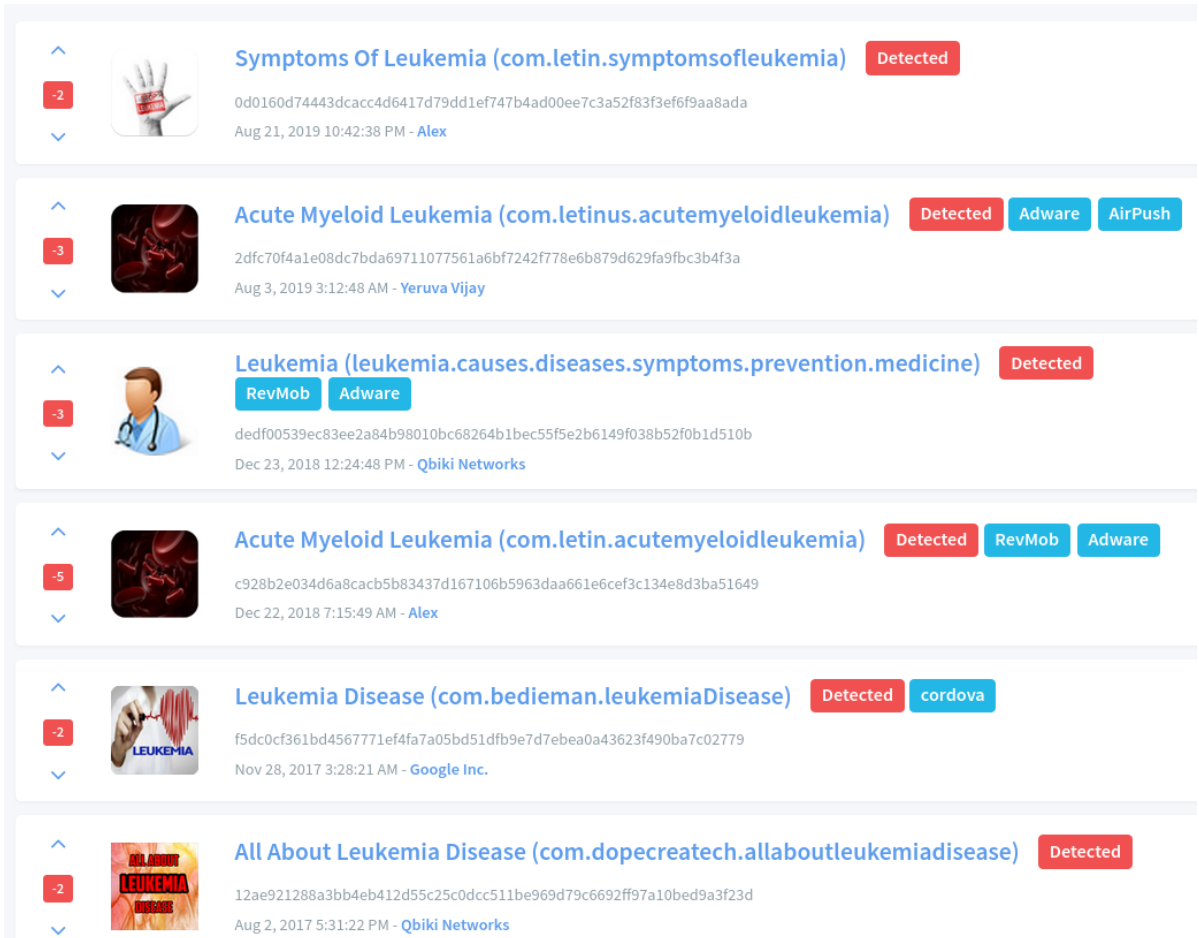
Malware in medical apps, fake apps etc



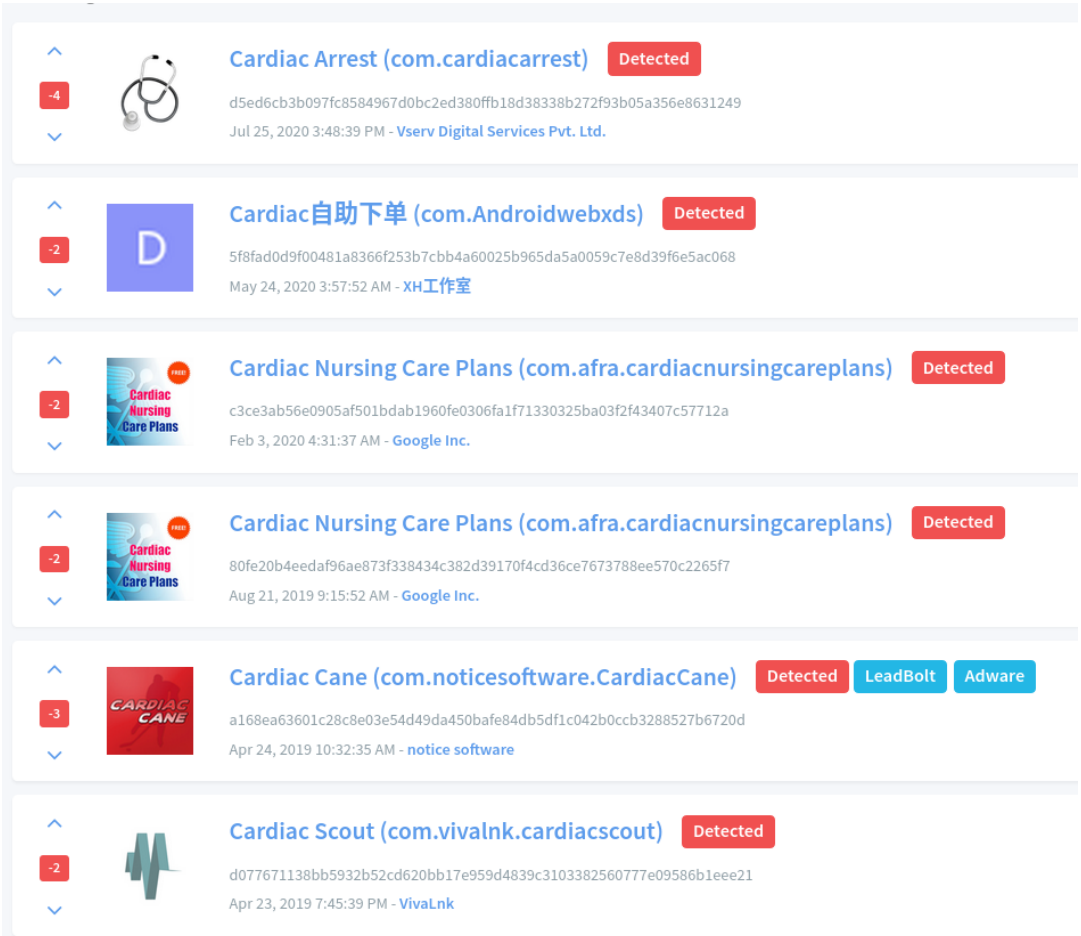
Malware in medical apps, fake apps etc



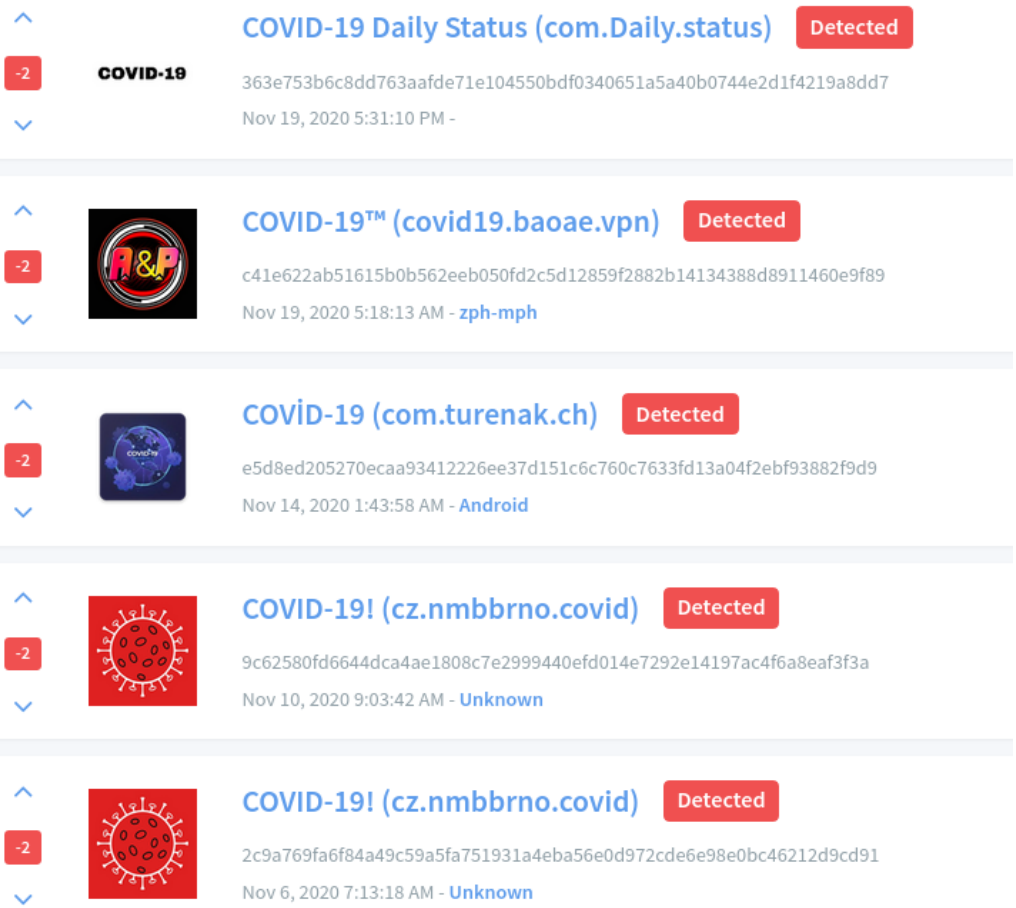
Malware in medical apps, fake apps etc



Malware in medical apps, fake apps etc



Malware in medical apps, fake apps etc



What are these malware in medical apps doing?

Lots of **adware**, **spyware**, **scams**...

Examples

- Communication to remote CnC
- File encryption (crypto locker)
- Ransomware
- Intercept, send, delete SMS
- Track geographic location
- Lock screen
- Screen capture
- Record audio
- Keylogger
- Grab current wallpaper
- Get battery level

Anything manipulating medical values or devices e.g remote control of an insulin pump? **No**. Fortunately not (but it could happen, especially for VIPs).

Compromised COVID-19 app

- In March 2020, an italian company developed a COVID-19 contact tracing app
- Several **malware repackaged the app** *"with metasploit"*
- sha256:

  7b8794ce2ff64a669d84f6157109b92f5ad17ac47dd330132a8e5de54d5d1afc
- Reference articles: Locating the trojan or How the malware works

Bibliography

- Reversing V-Alert COVID-19 (May 2020) or Aarogya Setu (Aug 2020) or SM-COVID (Sept 2020)
  https://cryptax.medium.com
- VB 2019:
  https://www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Apvrille-Lakhani.pdf
- Full report on malware in diabetes apps:
  https://fortinetweb.s3.amazonaws.com/fortiguard/research/diabetes-malware.pdf
- List of malware related to COVID-19:
  https://lukasstefanko.com/2020/03/android-coronavirus-malware.html

Thanks for your attention!

Axelle Apvrille
Email: aapvrille (at) fortinet (dot) com
Twitter: @cryptax

Ph0wn, a smart objects CTF: https://ph0wn.org

https://www.fortinet.com - https://fortiguard.com