

# Medical Malware on Android

a.k.a Android malware affecting medical apps

Axelle Apvrille

No Hat, November 28, 2020

## ① Introduction

Hello

Medical apps

Malware

## ② Live Reverse

Background info on the malware

# Hello! Who am I?



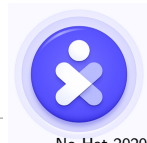
**Axelle Apvrille**

Principal Security Researcher at **Fortinet**, @cryptax  
Mobile malware, IoT, **Ph0wn CTF**

























# Lots of Medical Apps on Android



**COVID**  
Hôpitaux  
Universitaires  
de Marseille | ap·  
hm



# Malware in medical apps, fake apps etc





















  		<b>Diabetes Symtoms (com.v1_4.B88FE0CB7322E72EB287D61F.com)</b> <span>Detected</span> 9f2f88ba87836bd3eb734072ae32c492b4540f4def778eb206ae7fe8e4b3e437 Jul 26, 2020 12:47:27 AM -
  		<b>Signs of Diabetes (com.appman.signsofdiabetes)</b> <span>Detected</span> d3e7cc939576a4d49ddcb31027d544fb785ac4cb0f28767c093f9181372990 May 22, 2020 9:55:02 AM - <a href="#">Unknown</a>
  		<b>What Is Diabetes (com.a72256693652b2e87a0d8ec7a.a29761526a)</b> <span>Detected</span> 41b477b2c0adc28febebe105983bf129783536e1c0923a9e8509823910ab29c May 20, 2020 10:52:21 AM -
  		<b>Signs of Diabetes (com.appman.signsofdiabetes)</b> <span>Detected</span> b17aa3041a97a38e4c21c520867d2e918e55ac819390a550f12c45fd1833873d May 5, 2020 6:34:39 PM - <a href="#">Unknown</a>
  		<b>Trik Cegah Diabetes (com.TrikCegahDiabetes.sutriyanidroid)</b> <span>Detected</span> 6449df2a13198784cecbce530cf16f2dd53543b661c5c34db4ed11a55349a0 Apr 23, 2020 4:34:49 PM - <a href="#">individual</a>
  		<b>Gejala Diabetes (com.GejalaDiabetes.mardianadroid)</b> <span>Detected</span> cf85dbe1b93090c6181a799e57a10ec3ca136c3293f46774177b3e4b5ab0e6db Apr 21, 2020 7:05:30 PM - <a href="#">individu</a>

# Malware in medical apps, fake apps etc

The screenshot shows a list of six mobile applications. Each entry includes an icon, a title, a status (e.g., 'Detected'), a unique identifier, and a date. The apps are:


- Psychiatry (sk.psychiatry)**: Detected. Identifier: 33946db26a9cb1a72c9d17e443cca252102a4bd1084ed85d9d99bc0e456f403. Date: May 8, 2020 12:11:53 PM - Unknown.
- Psychiatry Guidelines DSM-5 (com.lobxrvsyldxgwz.psychiatryguidelinesdsm)**: Detected. Identifier: c46478fe804f192477c966a357677cc8933f4560c5e49ef8b01ca7a6a460e7c6. Date: Dec 20, 2018 8:16:40 AM - Brent.
- Child & Adolescent Psychiatry (com.uiewehjehjee.oirfofrlokff)**: Detected. Identifier: 23126a10400e4f51e549e7ce88a44e85f8e6d8bb8befd7d740347d9825664fb. Date: Aug 19, 2018 10:42:42 AM - Qbiki Networks.
- Psychiatry pocket (uk.lvesh.psychiatrypocket)**: Detected. Identifier: 2e201e7dd9b89b6762009abe462309a3cb3d3602c9cb8fb11c7552a3fd178dea. Date: Jul 16, 2017 1:42:53 AM - CL.
- The Maudsley Prescribing Guidelines in Psychiatry, 12th Edition (uk.abkvwio.themaudslprescribingguidelinesinpsychiatrythedition)**: Detected. Identifier: 58ccc4465457a71b3d31ff3b004f88b3d416653c0e0b7ba7678fb33616c3577e. Date: Mar 16, 2017 12:10:51 AM - Ryan.
- Psychiatry Guidelines DSM-5 (eu.trxekfaj.psychiatryguidelinesdsm)**: Detected. Identifier: fc7ed1b7a5a0efc3249b9adac24d83c6948d60c2b0c2e0a3a62e52a2b82efdec. Date: May 14, 2016 2:39:29 PM - Lori.

# Malware in medical apps, fake apps etc

  		<b>Chronic Fatigue Treatment (com.bestappsforphone.chronicfatiguesyndromecauses)</b> <span>Detected</span> 443ed6f783b577e3a06dd3449475b4c304e19e350b9c5089627485a26121a7a May 15, 2020 10:48:40 AM - <a href="#">Qbiki Networks</a>
  		<b>Chronic Fatigue Syndrome Cause (com.bestappsforphone.chronicfatiguesyndromecauses)</b> <span>Detected</span> 897d19691ca8fe1d2888f67140541476ba5d3dc781d19214653ded98702bf201 Apr 21, 2020 8:17:59 PM - <a href="#">Qbiki Networks</a>
  		<b>Holistic Chronic Pain Treatment (com.wHolisticChronicPainTreatment)</b> <span>Detected</span> ac83a8b138150735e206b4d4851870c1fd18e50f0511c8d5937204d0c0606242 Aug 6, 2019 9:03:37 AM - <a href="#">Kinal Miriam</a>
  		<b>Chronic Sinusitis (com.letin.chronicsinusitis)</b> <span>Detected</span> d3073f95749d214fae0636171e04e23ff165e18b2865ec40c01352b4b55e7996 Jul 30, 2019 12:39:01 AM - <a href="#">Alex</a>
  		<b>Chronic Bronchitis Information (com.biemultimedia.chronicbronchitisinformation)</b> <span>Detected</span> e6c145836e7f66deef7243c7c5688f3b9373cf209cdfa24cb1da21175a9f61aa Jun 9, 2019 10:07:24 AM - <a href="#">biemultimedia</a>

# Malware in medical apps, fake apps etc


↑  
-3  
↓

 Symptoms Of Leukemia (com.letin.symptomsofleukemia) Detected

0d0160d74443dacc4d6417d79dd1ef747b4ad00ee7c3a52f83f3ef69aaada  
Aug 21, 2019 10:42:38 PM - Alex

---


↑  
-3  
↓

 Acute Myeloid Leukemia (com.letinus.acutemyeloidleukemia) Detected Adware AirPush

2dfc70fa1e08dc7bd6e9711077561af8f7242f778e6b79d629fa9fbc3b4f3a  
Aug 3, 2019 3:12:48 AM - Yeruva Vijay

---


↑  
-3  
↓

 Leukemia (leukemia.causes.diseases.symptoms.prevention.medicine) Detected RevMob Adware

dcd00539ec83ee2a84b98010bc68264b1bec55f5e2b6149f038b52f0b1d510b  
Dec 23, 2018 12:24:48 PM - Qbiki Networks

---


↑  
-5  
↓

 Acute Myeloid Leukemia (com.letin.acutemyeloidleukemia) Detected RevMob Adware

c928b2e034d68cacb5b83437d167106b5963daa661e6cef3c134e8d3ba51649  
Dec 22, 2018 7:15:49 AM - Alex

---


↑  
-2  
↓

 Leukemia Disease (com.bedieman.leukemiaDisease) Detected cordova

f5dc0cf361bd456771ef4fa7a05bd51dfb9e7d7ebea0a43623f490ba7c02779  
Nov 28, 2017 3:28:21 AM - Google Inc.

---

↑  
-3  
↓

 All About Leukemia Disease (com.dopecreattech.allaboutleukemiadisease) Detected

12ae921288a3bb4eb412d55c25c0d0cc511be969d79c6692f97a10bed9a3f23d  
Aug 2, 2017 5:31:22 PM - Qbiki Networks



# Malware in medical apps, fake apps etc

The screenshot displays a list of five mobile applications, each with a rating, an icon, a title, a detection status, a unique identifier, and a release date. All applications are marked as 'Detected'.

- Cardiac Arrest (com.cardiacarrest)**: Detected. Rating: 4. Icon: Stethoscope. ID: d5ed6cb3b097fc8584967d0bc2ed380fb18d38338b272f93b05a356e8631249. Date: Jul 25, 2020 3:48:39 PM - Vserv Digital Services Pvt. Ltd.
- Cardiac自助下单 (com.Androidwebxds)**: Detected. Rating: 2. Icon: Blue square with 'D'. ID: 5f8fad0d9f00481a8366f253b7cbb4a60025b965da5a0059c7e8d396e5ac068. Date: May 24, 2020 3:57:52 AM - XH工作室
- Cardiac Nursing Care Plans (com.afra.cardiacnursingcareplans)**: Detected. Rating: 2. Icon: Cardiac Nursing Care Plans. ID: c3ce3ab56e0905af501bdab190fe0306fa1f71330325ba032f43407c57712a. Date: Feb 3, 2020 4:31:37 AM - Google Inc.
- Cardiac Nursing Care Plans (com.afra.cardiacnursingcareplans)**: Detected. Rating: 2. Icon: Cardiac Nursing Care Plans. ID: 80fc20b4eedaf96ae873f33843c382d39170f4cd35ce7673788ee570c2289f7. Date: Aug 21, 2019 9:15:52 AM - Google Inc.
- Cardiac Cane (com.noticesoftware.CardiacCane)**: Detected, LeadBolt, Adware. Rating: 3. Icon: Cardiac Cane. ID: a108ea63601c28c8e03e54d49da450baf6e4db5df1c042b0ccb3288527b6720d. Date: Apr 24, 2019 10:32:35 AM - notice software
- Cardiac Scout (com.vivalnk.cardiacscout)**: Detected. Rating: 3. Icon: ECG line. ID: d077671138bb5932b52c0620bb17e959d4839c3103382560777e09586b1eee21. Date: Apr 23, 2019 7:45:39 PM - VivaLink

# Malware in medical apps, fake apps etc

^

-2 COVID-19


COVID-19 Daily Status (com.Daily.status) **Detected**

363e753b6c8dd763aafde71e104550bdf0340651a5a40b0744e2d1f4219a8dd7

Nov 19, 2020 5:31:10 PM -

v

^

-2 


COVID-19™ (covid19.baoae.vpn) **Detected**

c41e622ab51615b0b562eeb050fd2c5d12859f2882b14134388d8911460e9f89

Nov 19, 2020 5:18:13 AM - [zph-mph](#)

v

^

-2 

COVID-19 (com.turenak.ch) **Detected**

e5d8ed205270ecaa93412226ee37d151c6c760c7633fd13a04f2ebf93882f9d9

Nov 14, 2020 1:43:58 AM - [Android](#)

v

^

-2 


COVID-19! (cz.nmbbrno.covid) **Detected**

9c62580fd6644dca4ae1808c7e2999440efd014e7292e14197ac4f6a8eaf3f3a

Nov 10, 2020 9:03:42 AM - [Unknown](#)

v

^

-2 

COVID-19! (cz.nmbbrno.covid) **Detected**

2c9a769fa6f84a49c59a5fa751931a4eba56e0d972cde6e98e0bc46212d9cd91

Nov 6, 2020 7:13:18 AM - [Unknown](#)

v

# 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).

## ① Introduction

Hello

Medical apps

Malware

## ② Live Reverse

Background info on the malware

# 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>