FORTINET

Medical Malware on Android

Axelle Apvrille

Nullcon webinar, August 2020

Hello! Who am I?

Axelle Apvrille

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

Mobile malware, IoT, Ph0wn CTF

Quiz no. 1 - End-user awareness

What would your family/ neighbours/ people in the street say?

Are there viruses on smartphones?

Quiz no. 1 - End-user awareness

What would your family/ neighbours/ people in the street say?

Are there viruses on smartphones?

Answer

Malicious Android *samples* - up to August 2020

Total: **6.3 million**

35,000 new **per day**

Quiz no.2

Are there mobile malware abusing of medical situations?

1. **No**. Apart pranks. Cybercriminals don't care if we have the flu, or whatever disease.
2. I heard of **a few mobile malware** related to **COVID-19**. . **Nothing before**. .
3. Cybercriminals attacked **numerous hospitals**. .
4. Hmmm. I think a cybercriminal **remotely controlled the pacemaker** of a US vice president, perhaps with a mobile phone?

Quiz no.2

Are there mobile malware abusing of medical situations?

1. **No**. Apart pranks. Wrong Cybercriminals don't care if we have the flu, or whatever disease. True
2. I heard of **a few mobile malware** related to **COVID-19**. . **Nothing before**. .
3. Cybercriminals attacked **numerous hospitals**. .
4. Hmmm. I think a cybercriminal **remotely controlled the pacemaker** of a US vice president, perhaps with a mobile phone?

Quiz no.2

Are there mobile malware abusing of medical situations?

1. **No**. Apart pranks. Wrong Cybercriminals don't care if we have the flu, or whatever disease. True
2. I heard of **a few mobile malware** related to **COVID-19**. True. **Nothing before**. Wrong.
3. Cybercriminals attacked **numerous hospitals**. .
4. Hmmm. I think a cybercriminal **remotely controlled the pacemaker** of a US vice president, perhaps with a mobile phone?

Quiz no.2

Are there mobile malware abusing of medical situations?

1. **No**. Apart pranks. Wrong Cybercriminals don't care if we have the flu, or whatever disease. True
2. I heard of **a few mobile malware** related to **COVID-19**. True. **Nothing before**. Wrong.
3. Cybercriminals attacked **numerous hospitals**. True, but not smartphones.
4. Hmmm. I think a cybercriminal **remotely controlled the pacemaker** of a US vice president, perhaps with a mobile phone?

Quiz no.2

Are there mobile malware abusing of medical situations?

1. **No**. Apart pranks. Wrong Cybercriminals don't care if we have the flu, or whatever disease. True
2. I heard of **a few mobile malware** related to **COVID-19**. True. **Nothing before**. Wrong.
3. Cybercriminals attacked **numerous hospitals**. True, but not smartphones.
4. Hmmm. I think a cybercriminal **remotely controlled the pacemaker** of a US vice president, perhaps with a mobile phone? Wrong. No known attack on Cheney. The rest is fiction (TV series *Homeland*).

When did we notice medical malware on Android?

Concern/Awareness rises in 2019
but we have reasons to believe it has existed for long

References:

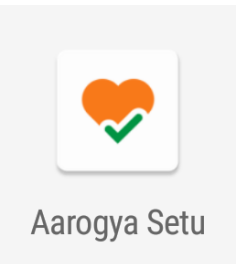
- VB 2019: https://www.virusbulletin.com/uploads/pdf/magazine/2019/VB2019-Apvrille-Lakhani.pdf
- Full report on diabetes malware: https://fortinetweb.s3.amazonaws.com/fortiguard/research/diabetes-malware.pdf

Mobile malware abuse COVID-19 apps / situation

Lists:

- https://lukasstefanko.com/2020/03/android-coronavirus-malware.html
- https://www.apklab.io/covid19
- Twitter: follow @fs0c131y
- Reversing V Alert Covid 19 (May 2020)

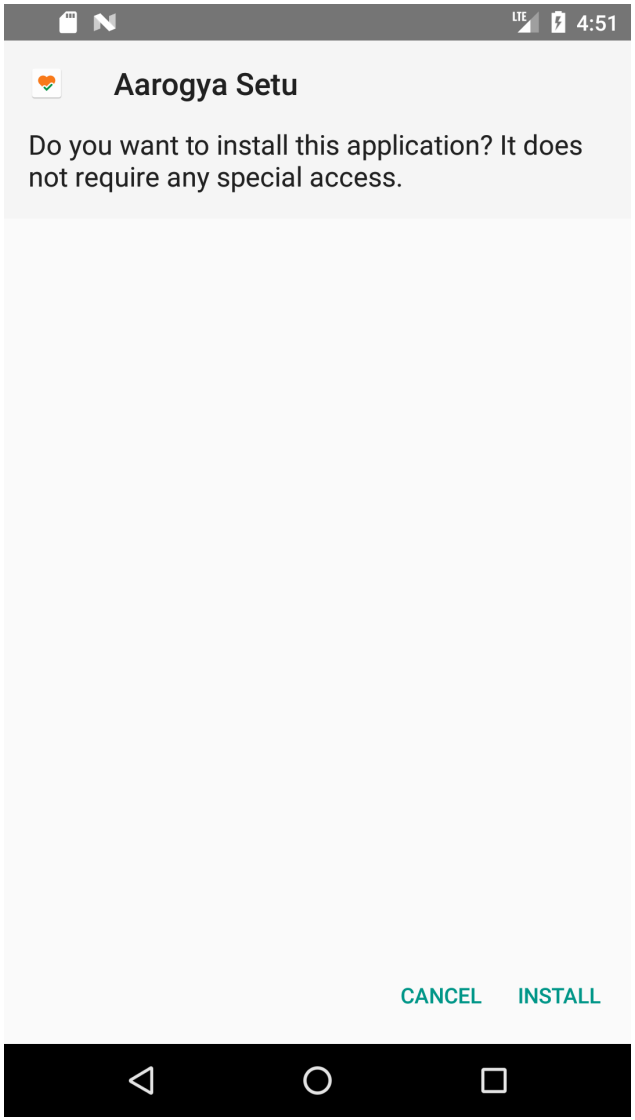
Fake Aarogya Setu app



- **Aarogya Setu** is the Indian open source COVID-19 contact tracing app
- There are **malicious fakes/copycats**
- sha256:

  885d07d1532dcce08ae8e0751793ec30ed0152eee3c1321e2d051b2f0e3fa3d7
- Full featured **spyware**
- Reference: my article on malware's CnC communication
- Detected as **Android/SpyAgent.APG!tr.spy** (aka SpyNote, SpyMax...)

Deceiving victims



Installs the real Aarogya Setu to deceive the victim

1. Victim thinks the app wasn't correctly installed yet, but the malware is already running
2. Victim only sees the icon (and app) of the real Aarogya Setu app, but the malware is installed and its icon is removed

Thanks for your attention!

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

Smart objects CTF: https://ph0wn.org

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