Reed Albergotti **@ReedAlbergotti** *Wed Apr 14 12:50:20 +0000 2021*

Thread: 1/12 The big scoop in this article with **@nakashimae** is we finally know all the details on how the FBI unlocked the iPhone belonging to a terrorist in the San Bernardino attacks in 2016. But it's even more interesting **https://t.co/kKSyvGgHjX**

2/12 The story also shines light on Apple's effort to control iPhone security in the same way it controls everything else about your phone, like the software you install, how you install and who gets paid for it

3/12 One surprising reveal: After the San Bernardino unlock, Apple tried to hire David Wang, the hacker at Azimuth security who wrote the exploit that unlocked the iPhone. Apple says it didn't know Azimuth was behind the unlock at the time

4/12 It makes sense, because Apple has hired or tried to hire many "jailbreakers" like Wang in an effort to erect an impenetrable wall around iOS to stop hackers

5/12 Later, Apple tried unsuccessfully to acquire Corellium, a company Wang co-founded. If you can't hire them or acquire them, you can always sue. That's what Apple did to Corellium, claiming a copyright violation. Apple nearly outed Azimuth's role in the unlock in that lawsuit

6/12 Corellium makes "virtual iPhones" for security researchers. If you have Corellium, you don't need a jailbroken iPhone to do security research. Apple thinks Corellium is bad, because the technology could end up in the wrong hands

7/12 Maybe security is the one area in which tight control is good for everyone. But maybe it's not. Tight control also means less transparency and less visibility into when and how hacks happen

8/12 The iPhone may be the most secure consumer product ever. As a result, ironically, we know very little about how many exploits exist for the iPhone and who is using them. We find out about zero-day exploits for iOS regularly. How many are out there that aren't reported?

9/12 The reason Apple believes Corellium is dangerous is that it allows researchers to examine that impenetrable wall Apple thinks can keep hackers out. Of course, examining the wall is also the only way to find flaws to fix

10/12 So what are we really talking about here? Making iOS more secure or making it appear to be impenetrable?

11/12 Apple said in the Corellium case that it wants security researchers to turn bugs into Apple because it's the right and moral thing to do. But Apple surely understands there is a market for this kind of research and people aren't going to give exploits away for free

12/12 If there is a market for iOS exploits, Apple should win. It's worth $2.25 trillion and has enough cash to outspend nearly anyone on paying for security exploits. It can hire whoever it wants. This isn't just about money or protecting iPhone customers. It's also about power