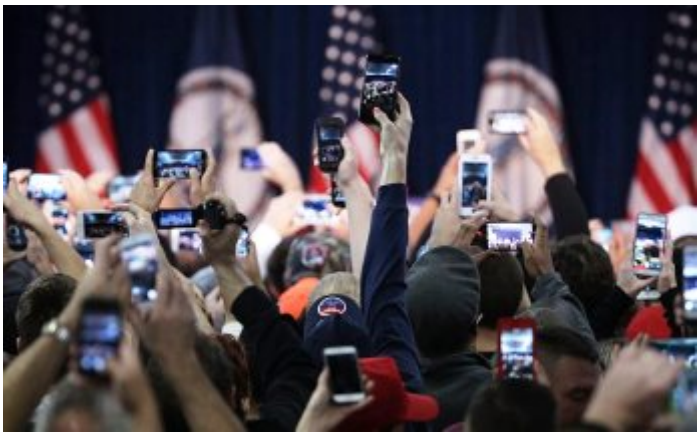
Smartphones - far too smart for the majority of users

by vax *Sunday, Aug 28 2016, 12:39am*
international / prose / post

> Indeed, the astounding features of smartphones are a juicy target for those interested in monitoring and surveillance, and I would add that not only government agencies (NSA) are involved in this type of hacking, private corporate hackers have exploited smartphones to rake in $zillions by selling their mal/spyware to any large entity that wishes to spy on its population.



Apple's reputation for 'security' -- now lost -- has indeed increased its iPhone/iPad sales, iPhones today are perhaps the most popular smartphones worldwide. But as an old hacker's axiom states, *"anything one man makes, another can break,"* and so it was inevitable that smartphones and other smart devices would be targeted and 'owned', as they are a treasure trove of saleable information, including location coordinates, remote text monitoring, recording and videoing etc, all done externally once security is breached by the click of a link, which associated code then secretly jailbreaks the phone and utilises ALL its functions, INVISIBLY.

I would add that the latest 'news' that iPhones have been hacked is not news at all, it's been going on for years, unpublished of course, after all, governments and hackers are not inclined to inform users they are being secretly watched. Corporate hackers also do not wish to kill the goose that laid the golden egg -- their private commercial spyware packages -- which they sell to anyone that has the mega-bucks to purchase them, which are usually socially oppressive and surveillance-addicted governments.

So are you safe, even with an upgrade? A rhetorical question, as you haven't been safe since you allowed governments and other interests (corporations) to engage in ILLEGAL pan-surveillance and other GROSS infringements on your personal rights and liberties -- so your cowardly complacence now serves you right, as it's now all out in the open, you have become exploited slaves with no privacy whatsoever by not asserting your democratic prerogatives when nefarious forces initially implemented their surveillance strategies under the guise of fighting 'terrorism/crime' -- talk about falling for a con, you lame, subservient, cowardly morons!

But it's never too late to restore your governments to REAL democracy which is representation that works in YOUR interests not the interests of mega-wealthy minorities that corrupt, poison and

destroy everything they touch, like FREEDOM for example!

All of Apple's once secure communications features are now an open book which the latest iOS patch MAY cure, but what of other UNDETECTED spywares, and there are plenty available on the dark web and in the mainstream corporate world. Of course available packages have varying degrees of effectiveness, a cheaper package may only remotely record your keystrokes and textual (email etc) comms, others may voice and video record, and of course what's it all worth without the ability to locate YOU almost anywhere in the world instantly, not forgetting the smart 'tapable' chips in your credit/smart cards, which monitor your movements and spending?

Your habits have become a RESOURCE that certain commercial interests pay huge amounts to posses, but what do you get? Sweet fuck all, except the loss of your identity, privacy and freedom? You are being exploited legally and illegally while I write, and I'm sure you haven't read the fine print which informs you of the fact that you are surrendering your freedom if you subscribe. Have you ever thought about demanding otherwise as a unified population which refuses to surrender it's most valued liberties? Probably not, too hard, thinking is also a strain these days - LOL!

Another option is of course the purchase of a limited capability mobile phone that doesn't GPS track, or voice/video record, roughly available at cost for under $5, think economies of scale to reduce this price to $1; indeed, many would purchase this type of unit, notwithstanding they would keep their smartphones for other narcissistic uses -- LOL!

Nevertheless, most people only want web capability (emails) and text messaging, and a smaller/tighter simple to use OS, with limited capability, which makes it far easier to secure and detect hacks.

Now think of guerrilla warfare tactics. Corporate and other hackers EXPLOIT the major IT companies which have done all the hard work by incorporating all these features into one pocket device, how convenient, as all 'we' have to do is hack, and where in. And don't complain people, you sold your arses decades back.

To conclude, nothing is secure, so the fewer features you have the more secure you are, I have never purchased or owned a smartphone the cheaper disposable models described above are fine and serve practical needs, though in some countries minimal ID is required for internet providers, so don't use your real ID as it's already a commodity for slave traders.

Forbes article follows:

> **Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text**
>
> Thomas Fox-Brewster
>
> NSO Group employees' lives must seem no different from others in the Israeli tech scene. They turn up every morning at their office in Herzelia, in Tel Aviv's northern district, take the lift in the plain looking complex – all grey and sandy exteriors – through smart card-lock doors and into to their similarly spartan offices. On the way they give a nod to their neighbours, fraud analysts from EMC-owned RSA, whose job it is to trawl the dark web for cybercriminals' latest escapades. They might even have time for a brief confab with staffers at their sister company, a secure smartphone designer. Then they settle down to code.

But for the last six years, their everyday routine has been nothing less than extraordinary: create the world's most invasive mobile spy kit without ever exposing their work. Now, though, they've been busted exploiting iPhones in some of the most astonishing attacks yet seen in the world of private espionage. The company, according to analyses from Citizen Lab and Lookout Mobile Security, discovered three previously-unknown and unpatched iOS vulnerabilities (known as zero-days) were exploited by the firm, with just one click of a link in a text required to silently jailbreak the phone. This allowed its malware, codenamed Pegasus, to install on the phone, hoovering up all communications and locations of the targeted iPhones. That includes iMessage, Gmail, Viber, Facebook, WhatsApp, Telegram and Skype communications, amongst other data. It can collect Wi-Fi passwords too.

Apple has now patched the flaws and released an update for iOS. A spokesperson said: "We were made aware of this vulnerability and immediately fixed it with iOS 9.3.5. We advise all of our customers to always download the latest version of iOS to protect themselves against potential security exploits."

Who are NSO Group?

NSO Group has been able to keep its surreptitious work under wraps until now. Previous articles only recorded their move into America and limited information on contracts: one allegedly for the former Panama president Ricardo Martinelli and another for Mexico. (Related note: I recently covered the story of Mayer Mizrachi, whose father is dating Martinelli's sister. Like Martinelli, Mizrachi is facing a corruption probe in Panama, but over alleged discrepancies with the WhatsApp rival, Criptext, he provided to the government).

Thanks to the analysis from Citizen Lab and Lookout, it's almost certain NSO also supplies to the United Arab Emirates (UAE). Ahmed Mansoor, an internationally-recognized human rights defender, alerted Citizen Lab researchers Bill Marczak and John Scott-Railton that his iPhone 6 was targeted on 10 August. They subsequently investigated the malware (full technical details of which can be found here and here), and within 10 days of being informed Apple issued the fix. The researchers later discovered Mexican journalist Rafael Cabrera had been targeted too. And looking at the domains registered by NSO, they determined Pegasus could have been used across Turkey, Israel, Thailand, Qatar, Kenya, Uzbekistan, Mozambique, Morocco, Yemen, Hungary, Saudi Arabia, Nigeria, and Bahrain, though there was no clear evidence.

A more comprehensive report from Business Insider.
