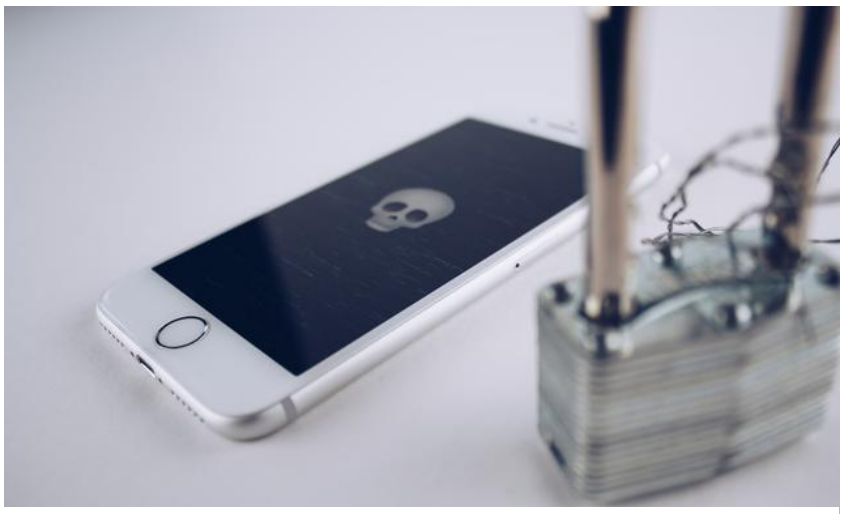
SCIENCE & TECH | #privacy | NEWS
Published on 21 July 2021, 05:50. Updated on 21 July 2021, 07:59.

Project Pegasus and the right to cultivate one's personal digital garden

by Achintya Rao



Credit: thoughtcatalog.com / Flickr

An investigation by a consortium of media outlets into Israel company NSO Group's Pegasus spyware has revealed politicians, journalists, human rights activists, and many others around the world as potential targets of widespread espionage. Geneva experts on cybersecurity and digital governance tell Geneva Solutions what citizens must do to stem the erosion of our right to privacy.

The leaked database of more than 50,000 phone numbers, including those belonging to French president Emmanuel Macron was first obtained by the Paris-based NGO Forbidden Stories, together with Amnesty International, who shared it with 17 media organisations around the world. The database shows potential targets of NSO clients whose mobile phones were to be infected by the Pegasus spyware.

Amid widespread condemnation, the UN High Commissioner for Human Rights, Michelle Bachelet, issued a statement yesterday, urging governments to "immediately cease their own use of surveillance technologies in ways that violate human rights, and [...]

take concrete actions to protect against such invasions of privacy by regulating the distribution, use and export of surveillance technology created by others".

So, what is Pegasus and whom does it target? "The software is a spying tool that is specialised in smartphones, namely iPhones, Androids and Blackberry devices," says Steven Meyer, an expert on cybersecurity and data protection, and CEO of ZENDATA, a cybersecurity firm based in Geneva. "It's very easy to install without needing physical access to the device. You don't necessarily need to know the person you're trying to infect or to have a direct contact with them." Once your phone is infected, Pegasus extracts a lot of information from it, recording all the content you have on your phone. It can easily spy on all your communications, record your screen, listen to your microphone and activate your camera.

What makes it particularly insidious is its ability to infect a phone without any action from the intended target. "This means of infection, maybe the most interesting one from a technical perspective, is what we call a 'zero-click' attack," Meyer explains. It exploits known vulnerabilities in the operating system on your phone. All an attacker has to do is initiate a WhatsApp call, for example, and the spyware installs itself without you even needing to answer the call.

"There's nothing trivial that you can do to protect yourself against this," Meyer continues. Short of swapping your latest smartphone for an older "feature phone", the previous generation of mobile phones with limited capabilities. "This is why Pegasus on the one hand is such a big success for people who want to spy and on the other hand a big concern for those who don't want to be spied upon. It's a very effective tool."

Means and intentions. But before you bin your favourite Apple and Google devices as a consequence of Pegasus, it is worth considering whom the software targets: "Pegasus is not something that everybody is going to be attacked with," Meyer says. "I don't know the price but I know it's very expensive and access to it is limited."

After all, there are easier ways for governments to use the basic set of features on smartphones to spy on foreigners and their own citizens alike. The Snowden revelations from nearly a decade ago demonstrated the ability of the companies we trust with our personal data to exploit that trust and hand over our information to the authorities without just cause. "I'm not going to create a panic attack, but when you buy an Android phone you have no control over what Google is doing with the contents of your phone," Meyer adds. "Even Apple, who advertise privacy, cannot technically prove that they are not violating your privacy; they cannot prove that one day if they change their minds to do it that they cannot do so retroactively."

Meyer does not believe that the companies are malicious. “But people who are purchasing Pegasus and are using it against someone have malicious intent. And this is where I think there is a big difference, between the intention and the means. Google and Apple have the means but not the intention, not as far as I am aware anyway. The people who use Pegasus have the intention and now with this tool they have the means, and this is where it gets scary.”

Professor Jovan Kurbalija, the founding director of the Diplo Foundation and the head of the Geneva Internet Platform, says that espionage, especially on an international level, is as old as humanity itself. “One of our deep drives is to see and not be seen.” What has changed in the digital age, however, is the extent to which espionage can target individuals, including private citizens.

Privacy versus spyware. Article 12 of the Universal Declaration of Human Rights enshrines an individual’s right to privacy. “The great philosopher Voltaire said in his book Candide that we should have our small gardens to cultivate,” notes Kurbalija. But rather than advocating for a detachment from the world, he makes the case for an online space that is both personal and private: “Today, we have to have our small digital gardens to cultivate, an intimate space in which we can be imperfect, who we are, as long as we don’t endanger anyone else.”

Kurbalija dismisses former Google boss Eric Schmidt’s infamous statement that if one had nothing to hide, one had nothing to fear. “We need privacy because it defines who we are as humans. And the more this type of spying there is, the more it endangers democratic processes and the very solidity of our social fabric.”

A common refrain from governments relying on spyware is that these tools are developed as counter-terrorism measures or to investigate violent crimes. After all, even though he likens spyware tools to weapons, Meyer is careful to remark that the NSO Group are not doing something illegal: “They’re making a product and they’re selling it. And when you hear about law enforcement arresting human traffickers by spying on their phones, it’s by using these kinds of tools. So just saying making such software is a no-go is too easy and not in line with reality.”

Kurbalija agrees. “The companies argue that they are producing security tools, and they are. But technology is only neutral until it is used; then it becomes for good or for bad.” And, he continues, while there have been a few attempts to ban espionage in international law, it remains legal when one state commits espionage against another. On top of which, and despite the universal desire for privacy, there remain differences in how cultures approach the subject. These would stand in the way of an umbrella international treaty governing spyware. The solution for regulating legal spyware may therefore be to treat it as dual-use technology, governed by the Wassenaar Agreement, Kurbalija suggests.

Protecting your digital garden. The revelations of Project Pegasus are nothing new, Meyer reminds us; it has been spoken about for a few years now. “I do think that it is a reminder to many that you shouldn’t assume your phone is as private as you want it to be.” At the same time, he warns against paranoia, suggesting that we continue to use our tools but be vigilant while doing so. For prime targets like dissident journalists, he proposes identifying the threat level and acting accordingly, taking advantage of a number of mitigation plans, including using feature phones or avoiding doing sensitive tasks on phones altogether.

There may be nothing to shield one from nefarious tools such as Pegasus. But, quoting Jean-Jacques Rousseau, Kurbalija says that countries have to revisit social contracts between ruled and rulers, what the rulers are allowed to do and what the ruled are comfortable with allowing. He extols individuals to raise the issue of our private digital garden as a political matter. “There will be two issues in my view which will determine our future: climate change and digital governance.”

#privacy #cybersecurity #digital governance