KCS Group Europe

The Pegasus Project: Secrets, lies, and mobile spies

11th August 2021

Pegasus, the spyware product designed by the Israeli surveillance company NSO has dominated the headlines since its exposure in July 2021. This is the third 'great leak' of recent times, after the Paradise and Panama Papers, and comes from the collaborative work of more than eighty journalists, from seventeen media organisations, in ten different countries. But unlike the first two leaks, which disclosed just how widespread the practice of hiding wealth & assets was, and the complicity of the political and corporate elite, Pegasus is about global surveillance operations designed to pick out the secrets of key political, journalistic and elite figures.

Given that this moves the frontier of surveillance and bad actors ever closer to the man-on-the-street, spectres of industrial espionage and state-sponsored monitoring of business targets must immediately loom larger than ever for the corporate world. Should you automatically assume that you have been compromised by Pegasus? What impact does this have on how you work? And given that despotic states are misusing this technology that was (allegedly) supposedly used only against terror targets, can a business looking to enter a foreign market that is in charitable terms, more 'complex', ever trust their local partners or government ever again?

The Pegasus Project uncovered that hundreds of people had been targeted for surveillance. This included world leaders, human rights activists, politicians, and journalists. More than fifty thousand telephone numbers were listed as potential targets of Pegasus. Whilst not all these numbers had yet been compromised, many had indeed contracted the spyware. Pegasus can penetrate both Apple and Android devices. Once infected, the spyware actively mines all data including but not limited to WhatsApp and text messaging, emails, contacts, call logs, images/vectors, location data, calendar, and videos. But it does not stop there. Pegasus can record calls, access your recorded messages inbox, activate your microphone, activate your camera, and access your password data. Moreover, Pegasus takes intelligent spyware to a new level with its 'zero click' ability to covertly embed itself within your device. This means, if it has found a vulnerability exploit onto your phone, it can self-activate regardless of whether you click the 'host' image, message, or link.

NSO firmly deny allegations of spying and distance themselves from any wrongdoing by squarely landing accountability of the use of the software by its 'clients'. Potential clients include (but not limited to) countries such as Saudi Arabia, UAE, Togo, Azerbaijan, Bahrain, Hungary, India, Mexico Morocco, Rwanda, and Kazakhstan. It is not clear how many people had suffered some sort of consequence in relation to being spied upon. It is clear however, of the few thus far known - as in the case of Saudi Journalist Jamal Khashoggi - the devastating outcome of real-world harm due to surveillance.

Khashoggi had been targeted with Pegasus (so too were his family), surveilled, located and assassinated. Khashoggi was murdered in Istanbul in October of 2018 after being lured on false pretences to collect papers from the consulate. NSO's argument appears to follow the car-crash argument: that, say, Mercedes cannot be blamed every time a Mercedes car crashes; it is the user of the product and not the manufacturer that is responsible. But this argument does not hold water, as a

Mercedes is not designed purely to crash into people. The sole function of Pegasus is to infiltrate onto private devices and take as much information as it can, expressly without consent. The 'new frontier' promised by technology is once again, receding to an authoritarian and elitist dominance where Big Brother is not only watching you, but listening to all of your conversations and reading your emails.

The extent of damage Pegasus has already inflicted and continues to wreak - used by state actors and individuals is not yet realised, and the true scope may never be known. Particularly in the business arena. Many businesses still view cybercrime and cyber espionage as 'someone else's problem'. Spying and corporate espionage is a multifaceted complex battlefield with which digital reconnaissance has the upper hand. How can spyware like Pegasus affect business? Such spyware can compromise cyber infrastructure - steal trade secrets, use designated high-level access to make changes to digital contracts, steal banking and client information, wreak relationship havoc then poach said clients. Businesses may suffer blackmail, extortion (the sale of data on the dark web), become vulnerable to fraud, and reputational damage.

Additionally, vulnerable employees may become compromised and high-level employees may even become exposed to real-world harm. Furthermore, there is a risk of spreading the spyware to clients creating a domino effect of compromise. Threat actors armed with potential new market entry information, may create a harsh business environment – exacerbating socio-political fragility.

We live in a 21st century digital era, where digital communications and the IoT's have become the fulcrum to our data driven world. But it is a double-edged sword. A digitalized world also provides unparalleled exploitative opportunities to the bad actor and OCG's. During 2020, more than half the population worldwide were online totalling nearly four billion users. More than 50 percent of the global population is connected to and using the internet excluding those who have access to it but seldom use it. To demonstrate the power of the internet, as of August 2020, there were ***42 million*** messages exchanged ***per minute*** using the WhatsApp platform alone. Our physical and digital worlds are symbiotic. World, business, and medicine infrastructure rely on digital communications and the IoT's. The fact that Pegasus is legally classified as a weapon by the Israeli state should come as no surprise. But just as few countries were willing to give up their nukes, so too should denials and reputations of Pegasus from state actors be met with equal scepticism. After all, nobody ever wanted to put the genie back into the lamp.