Pegasus Unveiled: The Cyber-Surveillance Weapon Of Scientific Dictatorship

Spyware supposedly under tight export control is now found to be a surveillance weapon of choice to track journalists and dissidents in autocratic nations. This is a chilling discovery that highlights how Technocrats have total control over surveillance. TN Editor

Human rights activists, journalists and lawyers across the world have been targeted by authoritarian governments using hacking software sold by the Israeli surveillance company NSO Group, according to an investigation into a massive data leak.

The investigation by the Guardian and 16 other media organisations suggests widespread and continuing abuse of NSO's hacking spyware, Pegasus, which the company insists is only intended for use against criminals and terrorists.

Pegasus is a malware that infects iPhones and Android devices to enable operators of the tool to extract messages, photos and emails, record calls and secretly activate microphones.

The leak contains a list of more than 50,000 phone numbers that, it is believed, have been identified as those of people of interest by clients of NSO since 2016.

Forbidden Stories, a Paris-based nonprofit media organisation, and Amnesty International initially had access to the leaked list and shared access with media partners as part of the Pegasus project, a reporting consortium.

The presence of a phone number in the data does not reveal whether a device was infected with Pegasus or subject to an attempted hack. However, the consortium believes the data is indicative of the potential targets NSO's government clients identified in advance of possible surveillance attempts.

Forensics analysis of a small number of phones whose numbers appeared on the leaked list also showed more than half had traces of the Pegasus spyware.

The Guardian and its media partners will be revealing the identities of people whose number appeared on the list in the coming days. They include hundreds of business executives, religious figures, academics, NGO employees, union officials and government officials, including cabinet ministers, presidents and prime ministers.

The list also contains the numbers of close family members of one country's ruler, suggesting the ruler may have instructed their intelligence agencies to explore the possibility of monitoring their own relatives.

The disclosures begin on Sunday, with the revelation that the numbers of more than 180 journalists are listed in the data, including reporters, editors and executives at the Financial Times, CNN, the New York Times, France 24, the Economist, Associated Press and Reuters.

The phone number of a freelance Mexican reporter, Cecilio Pineda Birto, was found in the list, apparently of interest to a Mexican client in the weeks leading up to his murder, when his killers were able to locate him at a carwash. His phone has never been found so no forensic analysis

has been possible to establish whether it was infected.

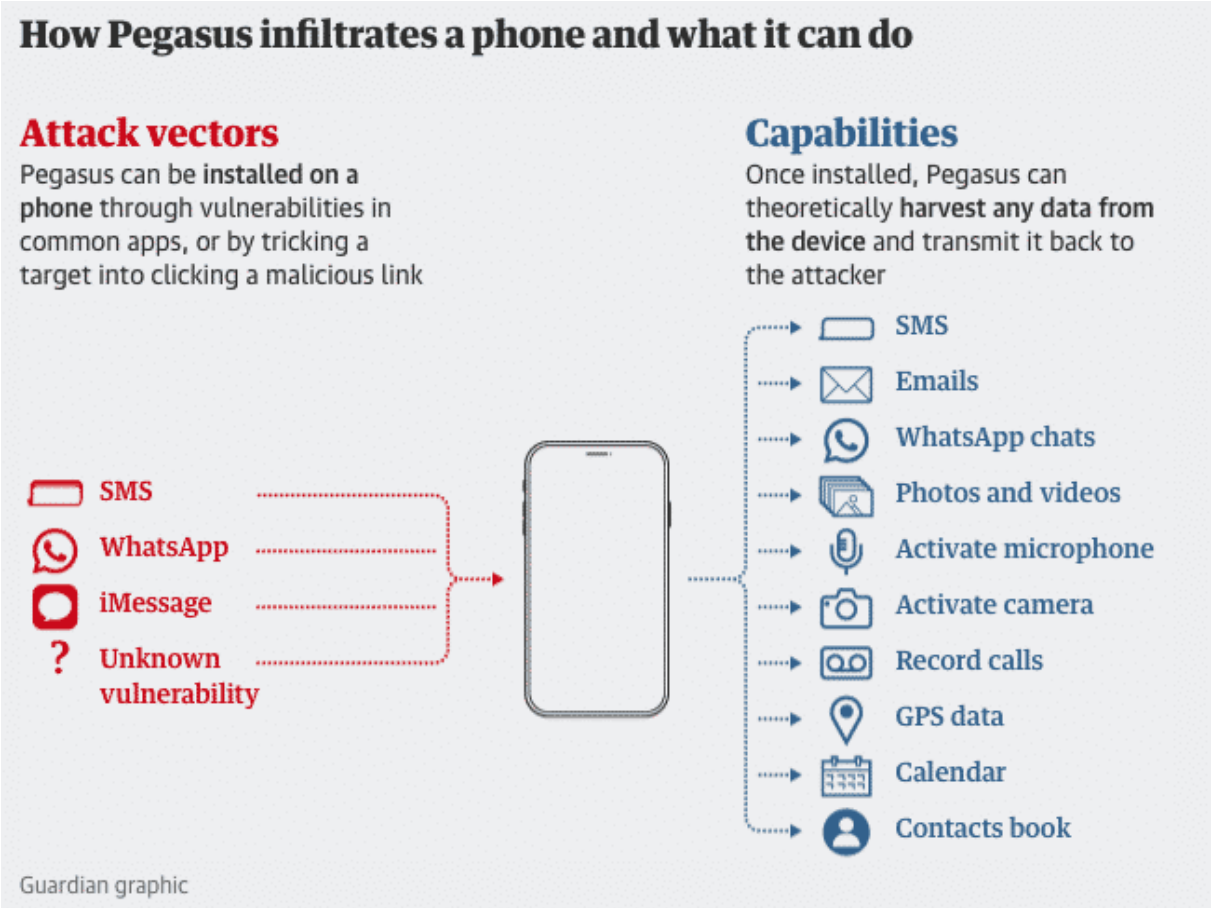
NSO said that even if Pineda's phone had been targeted, it did not mean data collected from his phone contributed in any way to his death, stressing governments could have discovered his location by other means. He was among at least 25 Mexican journalists apparently selected as candidates for surveillance over a two-year period.

Without forensic examination of mobile devices, it is impossible to say whether phones were subjected to an attempted or successful hack using Pegasus.

NSO has always maintained it "does not operate the systems that it sells to vetted government customers, and does not have access to the data of its customers' targets".

In statements issued through its lawyers, NSO denied "false claims" made about the activities of its clients, but said it would "continue to investigate all credible claims of misuse and take appropriate action". It said the list could not be a list of numbers "targeted by governments using Pegasus", and described the 50,000 figure as "exaggerated".

The company sells only to military, law enforcement and intelligence agencies in 40 unnamed countries, and says it rigorously vets its customers' human rights records before allowing them to use its spy tools.



Read full story here...