Israel spyware firm can mine data from social media

19 July 2019

Credit: CC0 Public Domain

An Israeli spyware firm thought to have hacked WhatsApp in the past has told clients it can scoop user data from the world's top social media, the *Financial Times* reported Friday.

The London paper wrote that NSO group had "told buyers its technology can surreptitiously scrape all of an individual's data from the servers of Apple, Google, Facebook, Amazon and Microsoft, according to people familiar with its sales pitch."

An NSO spokesperson, responding in a written statement to AFP's request for comment, denied the allegation.

"There is a fundamental misunderstanding of NSO, its services and technology," it said.

"NSO's products do not provide the type of collection capabilities and access to cloud applications, services, or infrastructure as listed and suggested in today's *FT* article."

In May, Facebook-owned WhatsApp said it had released an update to plug a security hole in its messaging app that allowed insertion of sophisticated spyware that could be used to spy on journalists, activists and others.

It said the attack bore "all the hallmarks of a private company that works with a number of governments around the world."

It did not name a suspect but Washington-based analyst Joseph Hall, chief technologist at the Center for Democracy and Technology, said at the time that the hack appeared related to the NSO's Pegasus software.

It is normally sold to law enforcement and intelligence services.

Friday's FT report, citing documents it had viewed and descriptions of a product demonstration, said the program had "evolved to capture the much greater trove of information stored beyond the phone in the cloud, such as a full history of a target's location data, archived messages or photos."

NSO says it does not operate the Pegasus system, only licensing it to closely vetted government users "for the sole purpose of preventing or investigating serious crime including terrorism."

The group came under the spotlight in 2016 when researchers accused it of helping spy on an activist in the United Arab Emirates.

NSO is based in the Israeli seaside hi-tech hub of Herzliya, near Tel Aviv. It says it employs 600 people in Israel and around the world.

Pegasus is a highly invasive tool that can reportedly switch on a target's cell phone camera and microphone, and access data on it, effectively turning the phone into a pocket spy.

"Increasingly sophisticated terrorists and criminals

are taking advantage of encrypted technologies to plan and conceal their crimes, leaving intelligence and law enforcement agencies in the dark and putting public safety and national security at risk," the company statement said.

"NSO's lawful interception products are designed to confront this challenge."