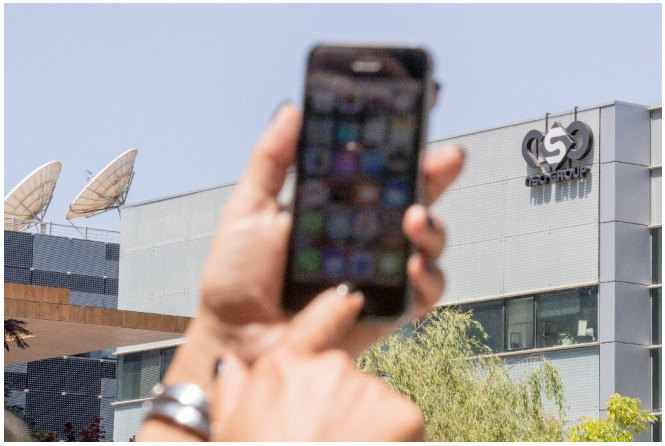
Israel spyware firm can mine data from social media: FT

19 July 2019



Spyware firm NSO is based in the Israeli seaside hi-tech hub of Herzliya, near Tel Aviv

An Israeli spyware firm thought to have hacked WhatsApp in the past denied a report Friday that it had boasted to clients that it can scoop user data from servers run by technology titans.

The Financial Times 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."

Amazon and Google told AFP that they were investigating the report, but had so far found no evidence that the software had breached their systems or customer accounts.

"We've found no evidence of access to Google accounts or systems, and we're continuing our investigation," a spokesman for the California-based internet giant said.

"We automatically protect users from security threats and we encourage them to use tools like our Security Checkup, 2-step verification, and our Advanced Protection Program, if they believe they may be at especially high risk of attack."

Amazon and Facebook stressed that customer security is a priority and that they were continuing to look into the claims.

"The best defence against this specific type of targeted attack is to maintain a healthy device," Microsoft senior director Jeff Jones said in response to an AFP inquiry, saying the firm's systems "are continually evolving to provide the best protections to our customers."

Cloud service users who suspect their smartphones or other devices have been compromised can reduce their risk with steps such as using account access "tokens" that expire after a short time, Jones said.

Apple did not immediately respond to a request for comment.

Tapping into smartphones

In May, Facebook-owned messaging app WhatsApp said it had released an update to plug a security hole that had allowed the 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.

The tool is normally sold to law enforcement and intelligence services.

The FT, citing documents it said it had viewed and descriptions of a product demonstration, said the programme 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".

If malware slipped onto a smartphone was capable of obtaining credentials people use to access cloud services, a hacker could conceivably access them too.

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 authorities spy on an activist in the United Arab Emirates.

NSO, based in the Israeli seaside hi-tech hub of Herzliya, near Tel Aviv, 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 as well as accessing data on the device, 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."