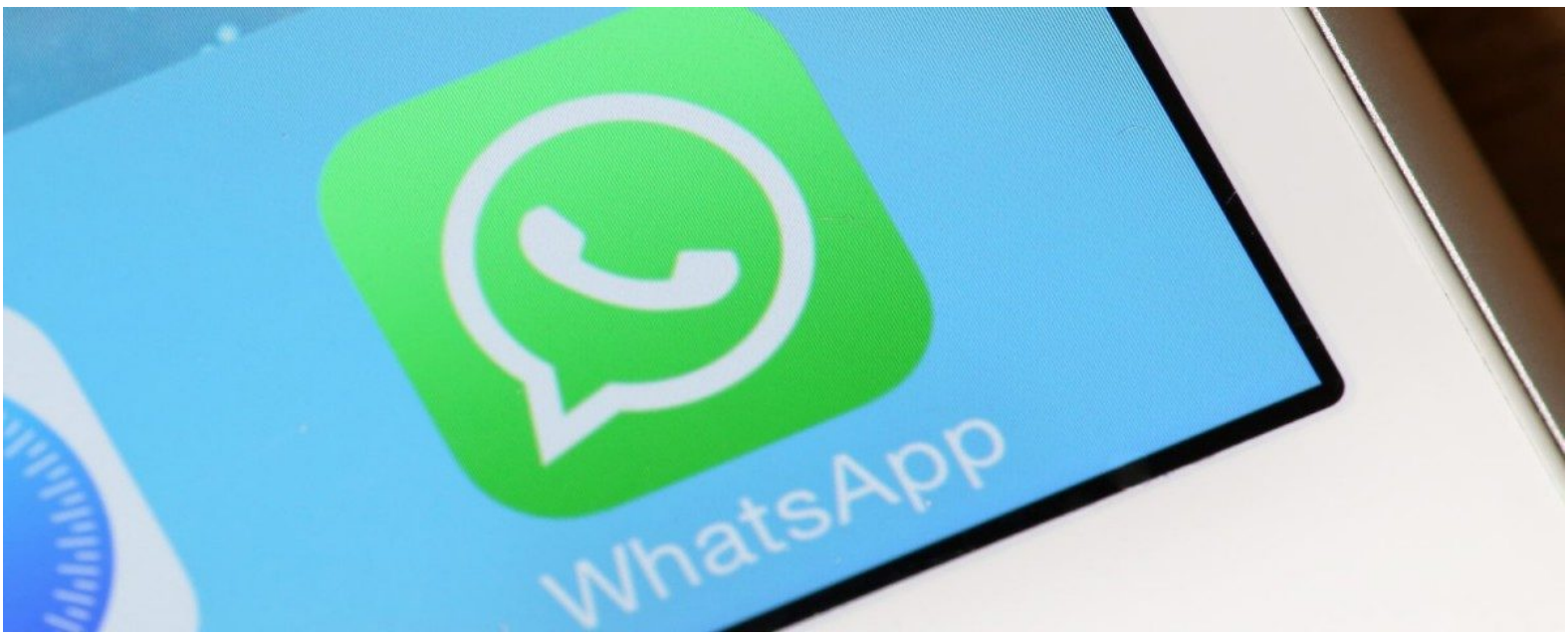
TECH

Israel Spyware Firm NSO Group Maintains Its Products 'Battle Terrorism' Alone

The creators of Pegasus, a spyware used to snoop on several journalists and lawyers associated with the Bhima Koregaon case, have said they have 'shut down' those who have abused their well-intentioned systems.



Israel's NSO Group had devised a hack that permitted it to intercept conversations conducted via WhatsApp. Source: Tim Reckman/Flickr (CC BY 2.0)

Lewis Sanders IV

RIGHTS TECH WORLD 10/FEB/2020

For years, Israel has been a cybersecurity powerhouse, with established companies and start-ups offering state-of-the-art services ranging from offensive cyber capabilities to AI-enabled defence systems.

Part of the reason for the industry's success is the active recruitment of military veterans and former agents of Israel's intelligence services. One of the most controversial companies to fall into this category is NSO Group, whose executives are believed to have served in Israel's elite signal intelligence-gathering Unit 8200.

Rights groups, press freedom advocates and even research hubs have accused the Herzliya-based company of turning a blind eye to the misuse of its security-oriented technology, including its contentious Pegasus spyware.

The most recent revelations have pointed to Saudi operators attempting to hack Amazon CEO Jeff Bezos' phone, although NSO Group has noted that it "can say unequivocally that our technology was not used in this instance."

Other instances have purportedly occurred, such as the targeting of activists from the Arab Gulf, North Africa and North America, including a close confidant of Saudi critic Jamal Khashoggi in the run-up to his assassination.

For security's sake

NSO Group's products are licensed for the sole purpose of fighting serious crime, combating terrorism and assisting in emergency search and rescue operations.

Also read: Israeli Spyware: Ask Not What Pegasus Does, But How Powerful Actors Operate in India

The company said that it had taken steps to prevent and discipline the misuse of its products, including putting in place a human rights policy and harmonising its governance structure in line with the UN Guiding Principles on Business and Human Rights.

“Customers are contractually obligated to cooperate in any investigation demanded from NSO Group and if misuse is confirmed, NSO Group has the ability to shut down their system and we have taken that step in the past,” a company spokesperson told DW.

Under its human rights policy, NSO Group acknowledges that while it has mechanisms to prevent the misuse of its software, its clients “should bear ultimate responsibility for the remedy of any harm to human rights.”

“We are incredibly proud of our products’ record of helping intelligence and law enforcement prevent serious crimes and save lives, but also understand that misuse could represent human rights violations,” said NSO Group CEO and co-founder Shalev Hulio last year.

“This new policy publicly affirms our equivocal respect for human rights and our commitment to mitigate the risk of misuse.”

But some believe that doesn’t go far enough.

For Danna Ingleton, deputy program director of Amnesty International’s technology division (Amnesty Tech), NSO Group needs to provide more details about how they have remedied the misuse of its technology.

“While, in theory, it is good that they have a human rights policy and are speaking about the importance of human rights, we need to see those words put to action,” Ingleton told DW.

Also read: Indian Activists, Lawyers Were ‘Targeted’ Using Israeli Spyware Pegasus

“So far we have no evidence that this human rights policy has changed the behaviour of the company, that it has resulted in them changing any of their due diligence practices or taking any of the complaints — legal or otherwise — about attacks or targeting of civil society seriously.”

Even in Israel, NSO Group is the target of legal action launched by 30 citizens, including members of the human rights community there. The case is aimed at revoking the company’s export license, which is granted by the Israeli Defense Ministry.

1 HOUR AGO

The Cisco Case Could Expose Rampant Prejudice Against Dalits in Silicon Valley

07 JUL

Examining the Legal and Policy Process Behind India's Ban on Chinese Apps

05 JUL

Chinese Apps: As Indian Video-Sharing Apps Capitalise on Ban, TikTok Distances Itself from Beijing

Ingleton, a trained lawyer, said the court case is one of the few ways to ensure NSO Group is held responsible.

“There was no avenue of redress when one of my Amnesty colleagues was targeted with NSO technologies and we hope this case will help remedy this situation,” Ingleton said.

Vulnerabilities

The discovery of a gaping flaw in Facebook-owned messaging app WhatsApp last year highlighted the misuse of NSO Group’s products. The vulnerability allowed an attacker to install spyware onto a targeted phone via a missed call on WhatsApp.

Facebook filed a lawsuit against NSO Group in October, accusing the Israeli company of providing foreign governments with the means to hack into 1,400 mobile phones across 20 countries. The California-based company said about 100 people involved in civil society work had been targeted.

However, by notifying users whose smartphones were compromised, Facebook had tipped off a terror suspect, The Wall Street Journal reported last month, citing a European law enforcement official.

In many ways, that is a prominent feature of such dual-use technologies; they present new opportunities and risks for civilians, authorities and the companies that make them. The challenge is finding the right balance.

This article first appeared on DW. *Read the original here.*

ALSO READ

05 JUL

Where Does India's Ban on Chinese Apps Fit Into the Global Trade Debate?

MORE