The New York Times | https://nyti.ms/2cfXAZy

TECHNOLOGY

How Spy Tech Firms Let Governments See Everything on a Smartphone

By NICOLE PERLROTH SEPT. 2, 2016

SAN FRANCISCO — Want to invisibly spy on 10 iPhone owners without their knowledge? Gather their every keystroke, sound, message and location? That will cost you $650,000, plus a $500,000 setup fee with an Israeli outfit called the NSO Group. You can spy on more people if you would like — just check out the company's price list.

The NSO Group is one of a number of companies that sell surveillance tools that can capture all the activity on a smartphone, like a user's location and personal contacts. These tools can even turn the phone into a secret recording device.

Since its founding six years ago, the NSO Group has kept a low profile. But last month, security researchers caught its spyware trying to gain access to the iPhone of a human rights activist in the United Arab Emirates. They also discovered a second target, a Mexican journalist who wrote about corruption in the Mexican government.

Now, internal NSO Group emails, contracts and commercial proposals obtained by The New York Times offer insight into how companies in this secretive digital surveillance industry operate. The emails and documents were provided by two people who have had dealings with the NSO Group but would not be named for fear of reprisals.

The company is one of dozens of digital spying outfits that track everything a target

does on a smartphone. They aggressively market their services to governments and law enforcement agencies around the world. The industry argues that this spying is necessary to track terrorists, kidnappers and drug lords. The NSO Group's corporate mission statement is "Make the world a safe place."

Ten people familiar with the company's sales, who refused to be identified, said that the NSO Group has a strict internal vetting process to determine who it will sell to. An ethics committee made up of employees and external counsel vets potential customers based on human rights rankings set by the World Bank and other global bodies. And to date, these people all said, NSO has yet to be denied an export license.

But critics note that the company's spyware has also been used to track journalists and human rights activists.

"There's no check on this," said Bill Marczak, a senior fellow at the Citizen Lab at the University of Toronto's Munk School of Global Affairs. "Once NSO's systems are sold, governments can essentially use them however they want. NSO can say they're trying to make the world a safer place, but they are also making the world a more surveilled place."

The NSO Group's capabilities are in higher demand now that companies like Apple, Facebook and Google are using stronger encryption to protect data in their systems, in the process making it harder for government agencies to track suspects.

The NSO Group's spyware finds ways around encryption by baiting targets to click unwittingly on texts containing malicious links or by exploiting previously undiscovered software flaws. It was taking advantage of three such flaws in Apple software — since fixed — when it was discovered by researchers last month.

The cyberarms industry typified by the NSO Group operates in a legal gray area, and it is often left to the companies to decide how far they are willing to dig into a target's personal life and what governments they will do business with. Israel has strict export controls for digital weaponry, but the country has never barred the sale of NSO Group technology.

Since it is privately held, not much is known about the NSO Group's finances,

but its business is clearly growing. Two years ago, the NSO Group sold a controlling stake in its business to Francisco Partners, a private equity firm based in San Francisco, for $120 million. Nearly a year later, Francisco Partners was exploring a sale of the company for 10 times that amount, according to two people approached by the firm but forbidden to speak about the discussions.

The company's internal documents detail pitches to countries throughout Europe and multimillion-dollar contracts with Mexico, which paid the NSO Group more than $15 million for three projects over three years, according to internal NSO Group emails dated in 2013.

"Our intelligence systems are subject to Mexico's relevant legislation and have legal authorization," Ricardo Alday, a spokesman for the Mexican embassy in Washington, said in an emailed statement. "They are not used against journalists or activists. All contracts with the federal government are done in accordance with the law."

Zamir Dahbash, an NSO Group spokesman, said that the sale of its spyware was restricted to authorized governments and that it was used solely for criminal and terrorist investigations. He declined to comment on whether the company would cease selling to the U.A.E. and Mexico after last week's disclosures.

For the last six years, the NSO Group's main product, a tracking system called Pegasus, has been used by a growing number of government agencies to target a range of smartphones — including iPhones, Androids, and BlackBerry and Symbian systems — without leaving a trace.

Among the Pegasus system's capabilities, NSO Group contracts assert, are the abilities to extract text messages, contact lists, calendar records, emails, instant messages and GPS locations. One capability that the NSO Group calls "room tap" can gather sounds in and around the room, using the phone's own microphone.

Pegasus can use the camera to take snapshots or screen grabs. It can deny the phone access to certain websites and applications, and it can grab search histories or anything viewed with the phone's web browser. And all of the data can be sent back to the agency's server in real time.

In its commercial proposals, the NSO Group asserts that its tracking software and hardware can install itself in any number of ways, including "over the air stealth installation," tailored text messages and emails, through public Wi-Fi hot spots rigged to secretly install NSO Group software, or the old-fashioned way, by spies in person.

Much like a traditional software company, the NSO Group prices its surveillance tools by the number of targets, starting with a flat $500,000 installation fee. To spy on 10 iPhone users, NSO charges government agencies $650,000; $650,000 for 10 Android users; $500,000 for five BlackBerry users; or $300,000 for five Symbian users — on top of the setup fee, according to one commercial proposal.

You can pay for more targets. One hundred additional targets will cost $800,000, 50 extra targets cost $500,000, 20 extra will cost $250,000 and 10 extra costs $150,000, according to an NSO Group commercial proposal. There is an annual system maintenance fee of 17 percent of the total price every year thereafter.

What that gets you, NSO Group documents say, is "unlimited access to a target's mobile devices." In short, the company says: You can "remotely and covertly collect information about your target's relationships, location, phone calls, plans and activities — whenever and wherever they are."

And, its proposal adds, "It leaves no traces whatsoever."

A version of this article appears in print on September 3, 2016, on Page A1 of the New York edition with the headline: Phone Spying Is Made Easy. Choose a Plan.
