The Moscow Times
30 YEARS
INDEPENDENT NEWS FROM RUSSIA

Why Is Russia Not Using Pegasus Spyware?

Pegasus spyware leak appears to vindicate FSB's paranoia concerning foreign-made surveillance technology.

By Andrei Soldatov

July 21, 2021

EPA / TASS

When a group of international investigative journalists and researchers broke the news that spyware called Pegasus, produced by the Israeli NSO Group, had helped repressive governments across the world spy on journalists, activists and lawyers on an unprecedented scale, the question emerged: Where was Russia?

Russia's government bodies — the secret services — are known to actively spy on journalists, activists, and lawyers. The NSO Group said it only sold spyware to vetted government bodies, not to private actors. And the relationship between Israel and Russia has been sufficiently close for years. So why is the FSB, or any other Russian agency, not on the list of NSO clients?

It is a good question — one my colleagues and I have been asking ourselves for almost a decade.

In October 2012, British NGO Privacy International, Canadian Citizen Lab and our website, Agentura.Ru, launched a joint project called "Russia's Surveillance State" to look into surveillance practices in Russia, including trade in surveillance technology. Part of our aim was to find out what kind of foreign surveillance hardware and software was being imported into Russia.

Related article: Russia, Belarus Spy Agencies Join Forces Against 'Destructive' West

We had assembled a dream team for the task. Privacy International had the best people to track down the contracts and agreements between the world's top surveillance equipment manufacturers and repressive governments, while Citizen Lab is a leader in detecting malicious code implanted on activists' devices.

What we learned was not exactly what we had expected.

Russia indeed had participated in trading global spy tech. Russian technology has been exported to regimes in South America and the Middle East, not to mention in Central Asia.

In many post-Soviet republics, Russian-made SORM black boxes have been intercepting communications, while in Mexico, Russian-made voice recognition technology has been used on a national scale to identify people based on intercepted phone calls since 2008.

Israel and Russia also have a history of technical cooperation. STT group, the biggest Russian developer of "engineer reconnaissance solutions" sells its equipment to Israel. It's used by combat engineers to enable forward movement of military troops by checking minefields, bridges and logging obstacles.

Related article: The Latest Spy Scandal Won't Sour Moscow-Rome Relations, But Italian Public Opinion Is Shifting

But Russia's government agencies do not buy foreign-made spyware.

On the world market for espionage technology, Russia is a seller, not a buyer.

Russian spy masters are proud successors to a long tradition of excellent intelligence technology, first developed under Joseph Stalin. They include famous inventions such as the Great Seal bug, a listening device concealed inside a gift given by the Soviet Union to W. Averell Harriman, U.S. Ambassador, and used to spy on the American ambassadors in Moscow for seven years.

The technology being used today to identify Mexican phone users was developed by a company which is a direct successor to a Soviet-era *sharashka* — the top secret military research and development labs based in Gulag prison camps, where detained academics and scientists, such as Aleksandr Solzhenitsyn, were forced to work.

But that Russian technology is generally very good is only part of the reason why Russian spies aren't buyers on the global market.

The FSB is also extremely paranoid about foreign spyware.

The FSB suspects — for good reason — that foreign developers cooperate with the intelligence agencies of their home countries, and that once any equipment is acquired through them, it could provide those foreign intelligence services with a decent chance of penetrating and compromising Russia's operations.

Looking into the way Pegasus operates, this concern seems to be justified. The NSO Group sells Pegasus mobile phone spyware to government agencies as a product, but when it is put to use, things get tricky.

To monitor a target, a government agency must convince the target to click on a special link, which, when clicked, installs Pegasus without the user's knowledge.

But once Pegasus is installed, it begins contacting the Pegasus' so-called command and control (C&C) servers. And these servers are often manned not by spy agencies, but are part of the Pegasus ecosystem.

That means Pegasus' creators, the NSO Group, are ideally positioned to also collect data from the targets that its clients — secret service agencies all over the world — are spying on. This information is an intelligence goldmine, and Russian secret services have never wanted to share this kind of data with outsiders.

The investigation into Pegasus was prompted by a leak of a list containing over 50,000 phone numbers that had likely been identified as people of interest to NSO's clients.

That suggests the targets of surveillance in multiple countries were compiled into one list, and this list was maintained not by the spy agencies, but by NSO itself.

And after all, who could blame the FSB for being paranoid after such a leak?

The views expressed in opinion pieces do not necessarily reflect the position of The Moscow Times.

Original url:
https://www.themoscowtimes.com/2021/07/21/why-is-russia-not-using-pegasus-spyware-a74572