US sanctions four companies selling hacking tools, including NSO Group & Candiru

By Catalin Cimpanu

Published: 2022-12-18 · Archived: 2026-04-05 13:08:07 UTC

The US government has sanctioned today four companies that develop and sell spyware and other hacking tools, the US Department of Commerce announced today.

The four companies include Israel's **NSO Group** and **Candiru**, Russian security firm **Positive Technologies**, and Singapore-based **Computer Security Initiative Consultancy**.

US officials said the four companies engaged in "activities that are contrary to the national security or foreign policy interests of the United States."

Commerce officials said NSO Group and Candiru "developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers."

The US said these tools were abused by foreign governments to conduct trans-national repression of dissidents, journalists, and activists outside of those governments' sovereign borders.

Similarly, Positive Technologies and CSIC were accused of creating and selling "cyber tools" that were later used to hack individuals and organizations worldwide.

Country	Entity	License requirement	License review policy	Federal Register citation
*******				
ISRAEL	*******			
	Candiru, a.k.a., the following seven aliases: -Candiru Ltd.; -DF Associates Ltd.; -Grindavik Solutions Ltd.; -Taveta Ltd.; -Saito Tech Ltd.; -Greenwick Solutions; *and* -Tabatha Ltd. 21 Haarbaa, Tel Aviv-Yafo, Israel 6473921.	All items subject to the EAR. (See §744.11 of the EAR).	Presumption of denial.	86 FR [INSERT FR PAGE NUMBER AND DATE OF PUBLICATION IN THE FEDERAL REGISTER].
	*******			
	NSO Group, 22 Galgalei Haplada, Herzliya, Tel Aviv-Yafo, Israel 4672222.	All items subject to the EAR. (See §744.11 of the EAR).	Presumption of denial.	86 FR [INSERT FR PAGE NUMBER AND DATE OF PUBLICATION IN THE FEDERAL REGISTER].
	*******			
*******				
RUSSIA	*******			
	Positive Technologies, 8 Preobrzhenskaya Square, Moscow, Russia, 107061.	All items subject to the EAR. (See §744.11 of the EAR).	Presumption of denial.	86 FR [INSERT FR PAGE NUMBER AND DATE OF PUBLICATION IN THE FEDERAL REGISTER].
	*******			
*******				
SINGAPORE	*******			
	Computer Security Initiative Consultancy PTE. LTD., a.k.a., the following alias: -COSEINC. 102F Pasir Panjang Rd, #08-02, Citilink Warehouse Complex, Singapore 118530.	All items subject to the EAR. (See §744.11 of the EAR).	Presumption of denial.	86 FR [INSERT FR PAGE NUMBER AND DATE OF PUBLICATION IN THE FEDERAL REGISTER].
	*******			
*******				

The four companies, including their aliases (detailed in the table above), were added to a list of entities engaging in malicious cyber activities that is currently maintained by the Commerce Department's Bureau of Industry and Security (BIS).

US companies and agencies must obtain a special license from BIS before buying, exporting, or transferring any cyber tools developed by the four companies. Commerce officials said that all applicants should expect a "presumption of denial" when applying for this license.

The sanctions today will make it harder for any of these companies to work with US individuals and contractors, limiting the four's ability to work with US-based partners.

"Today's action is a part of the Biden-Harris Administration's efforts to put human rights at the center of US foreign policy, including by working to stem the proliferation of digital tools used for repression," the Department of Commerce said in a press release today, announcing its decision.

The Department of Commerce did not reveal the finer points and evidence it used to sanction the four companies, but for three of the four sanctioned companies, there's been some public reporting of how their hacking tools have been abused over the past few years:

- **NSO Group** developed the Pegasus hacking platform, which the company rents to foreign governments. Pegasus abuses have been very well documented across the years.
- **Candiru** was recently exposed in reports by Microsoft and Citizen Lab as the creators of the DevilsEye Windows spyware. The company's hack-for-hire offerings have been known for years, and the company is also believed to have also developed and sold zero-day exploits for Chrome, Internet Explorer, and Windows.
- **Positive Technologies** has been accused of having developed and sold exploits to Russian intelligence agencies. The company was already under US Treasury sanctions since April this year.

Fewer details are available about Singapore-based CSIC, but the company is known for running an exploit acquisition program named Pwn0rama. There is currently no public reporting linking exploits bought via this program to known attacks, however, sources familiar with the exploit brokerage market have told *The Record* that the company has close ties to the Chinese market.

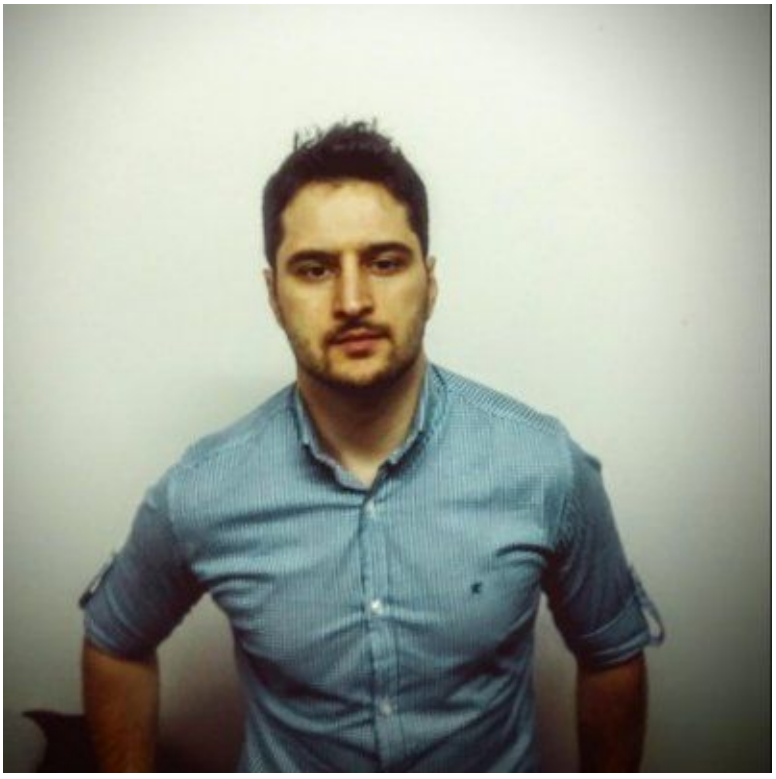
The Record has sent requests for comment on today's sanctions to Positive Technologies, CSIC, and NSO Group. No contact details were available for Candiru. The NSO Group has provided the following statement:

> NSO Group is dismayed by the decision given that our technologies support US national security interests and policies by preventing terrorism and crime, and thus we will advocate for this decision to be reversed.
>
> We look forward to presenting the full information regarding how we have the world's most rigorous compliance and human rights programs that are based the American values we deeply share, which already resulted in multiple terminations of contacts with government agencies that misused our products.
>
> *NSO spokesperson*

Article updated with NSO Group statement.

No previous article

No new articles



Catalin Cimpanu

is a cybersecurity reporter who previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.
