

Israeli Spyware Firm QuaDream Linked to Hacks on Journalists and Politicians

Cyber watchdog says spyware developed by a little-known firm used to hack devices across 10 countries

By [Middle East Eye](#)

Global Research, April 13, 2023

[Middle East Eye](#) 12 April 2023

Region: [Middle East & North Africa](#)

Theme: [Intelligence](#)

All Global Research articles can be read in 51 languages by activating the Translate Website button below the author's name.

To receive Global Research's Daily Newsletter (selected articles), [click here](#).

Click the share button above to email/forward this article to your friends and colleagues. Follow us on [Instagram](#) and [Twitter](#) and subscribe to our [Telegram Channel](#). Feel free to repost and share widely Global Research articles.

An [Israeli](#)-made spyware resembling the controversial Pegasus programme has been used to target journalists and opposition politicians in at least ten countries around the world, researchers have found.

The little-known Israeli vendor named QuaDream, which markets spyware under the name "Reign", was established by a former Israeli military official and veterans of the [NSO Group](#), the creator of Pegasus, cybersecurity researchers from Citizen Lab at the University of Toronto [said](#) on Tuesday.

According to the researchers, QuaDream prefers to keep a low profile and has largely avoided the limelight, in contrast with its competitor, Israel's NSO Group.

Unlike the NSO Group, which was blacklisted by the US in 2021 for its ties to illegal surveillance programmes, QuaDream has escaped scrutiny, until now.

Reign's "Premium Collection" capabilities included "real-time call recordings, camera activation - front and back," and "microphone activation," according to a company brochure uncovered by Citizen Lab.

QuaDream has sold its products to a range of government clients including the [United Arab Emirates](#), [Saudi Arabia](#), Mexico, and Ghana, and has pitched its services to Indonesia and [Morocco](#).

As part of its strategy to avoid the pitfalls that the NSO Group faced, QuaDream operates with a minimal public presence, meaning no website, no media coverage, and no social

media presence.

The attacks launched by QuaDream compromised phones running iOS 14, a state-of-the-art iPhone operating system, between 2020 and 2021.

The attacks were connected to calendar invitations and worked without user interaction, which is considered as a “zero click” attack.

“The firm has common roots with NSO Group, as well as other companies in the Israeli commercial spyware industry, and the Israeli government’s own intelligence agencies,” Citizen Lab said.

Last year Reuters [reported](#) that NSO and Reign at one point both exploited the same iOS bug to hack into devices.

Mounting legal woes

Israel has faced repeated criticism and diplomatic pressure over spyware and other cyber weapons being developed in the country.

Last month, the White House said that Pegasus has been used by governments “to facilitate repression and enable human rights abuses”.

In December 2022, a prominent [Bahraini](#) activist and blogger, the UK-based dissident Yusuf al-Jamri, [started legal action](#) against the NSO Group over allegations that his phone was hacked with [Pegasus](#).

Four other UK-based Arab dissidents have [also taken legal action](#) this year against the NSO Group, Saudi Arabia and the UAE over allegations that they were targeted with Pegasus.

The Pegasus software has been used by governments, including [Morocco](#), [Saudi Arabia](#), and the UAE, to illegally access the phone data of activists and journalists worldwide.

In 2021, Amnesty International obtained a leaked database of 50,000 phone numbers selected by NSO Group clients. The reporting revealed the widespread and international use of spyware to target politicians, activists and journalists.

The US Supreme Court in January allowed Meta Platforms Inc’s WhatsApp to pursue a lawsuit against NSO Group for exploiting a bug in the messaging app that installed spy software, enabling the surveillance of hundreds of people, including journalists, human rights activists, and dissidents.

WhatsApp – owned by Meta (formerly Facebook) – filed its lawsuit against the NSO Group in 2019, accusing the company of allegedly targeting its servers in California with malware to gain unauthorised access to approximately 1,400 mobile devices in violation of US state and federal law.

Last year, the Biden administration placed the NSO Group on an “Entity List” of companies considered to be engaged in activities contrary to US foreign policy and national security. The administration accused it of enabling “transnational repression” with its spyware.

NSO also faces a lawsuit from Apple, which claims the spyware maker violated US laws by

breaking into the software installed on its iPhones.

*

Note to readers: Please click the share button above. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

Featured image is from TruePublica

The original source of this article is [Middle East Eye](#)
Copyright © [Middle East Eye](#), [Middle East Eye](#), 2023

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Middle East Eye](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca
www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca