U.S. sanctions Predator spyware operators for spying on Americans

By Bill Toulas

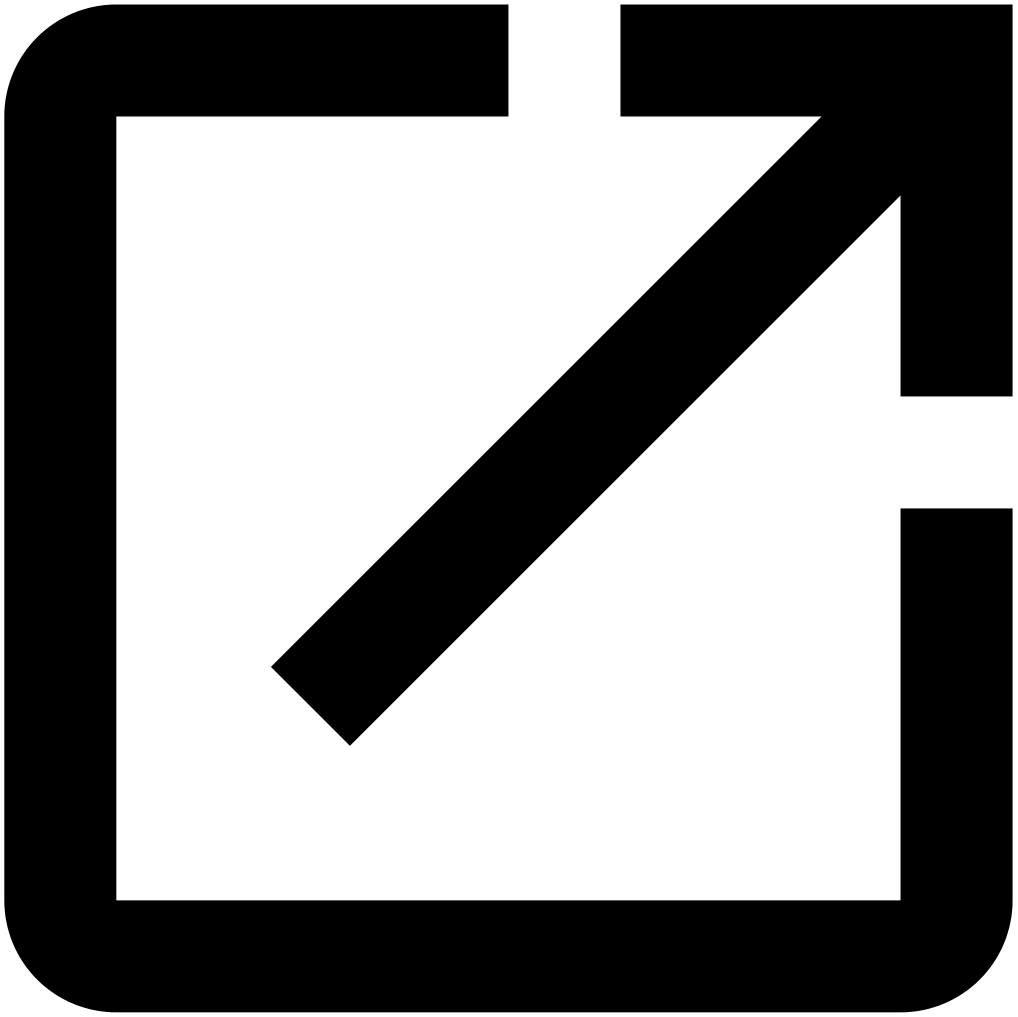
Published: 2024-03-05 · Archived: 2026-04-05 14:11:38 UTC

The U.S. has imposed sanctions on two individuals and five entities linked to the development and distribution of the Predator commercial spyware used to target Americans, including government officials and journalists.

"Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) designated two individuals and five entities associated with the Intellexa Consortium for their role in developing, operating, and distributing commercial spyware technology used to target Americans, including U.S. government officials, journalists, and policy experts," reads a press release by the Office of Foreign Assets Control (OFAC).

The sanctions target Intellexa Consortium's Israeli founder, **Tal Jonathan Dilian**, and Polish corporate specialist, **Sara Aleksandra Fayssal Hamou**.


DIE LINKE.
0:00



Visit Advertiser websiteGO TO PAGE

The sanctioned companies that are linked to spyware tech distribution are:

1. **Cytrox AD** – North Macedonia
2. **Cytrox Holdings Zartkoruen Mukodo Reszvenytarsasag (Cytrox Holdings ZRT)** – Hungary
3. **Intellexa Limited** – Ireland
4. **Intellexa S.A.** - Greece
5. **Thalestris Limited** – Ireland

Intellexa's commercial spyware technologies, specifically a product named 'Predator,' have been used to target key persons worldwide, including the United States. The attacks have enabled human rights abuses and the targeting of dissidents by oppressive regimes or state-sponsored cyberespionage by governments.

Common targets of Predator include government officials, journalists, politicians, activists, policy experts, and even high-ranking tech firm executives, with more details about Predator's targets found here.

Intellexa was also highlighted in a recent Google report where researchers warned the company utilizes zero-day vulnerability to install the spyware. In 2022, Google's Threat Analysis Group (TAG) reported that Predator was using zero-day vulnerabilities in Chrome and Android to infect fully-patched phones.

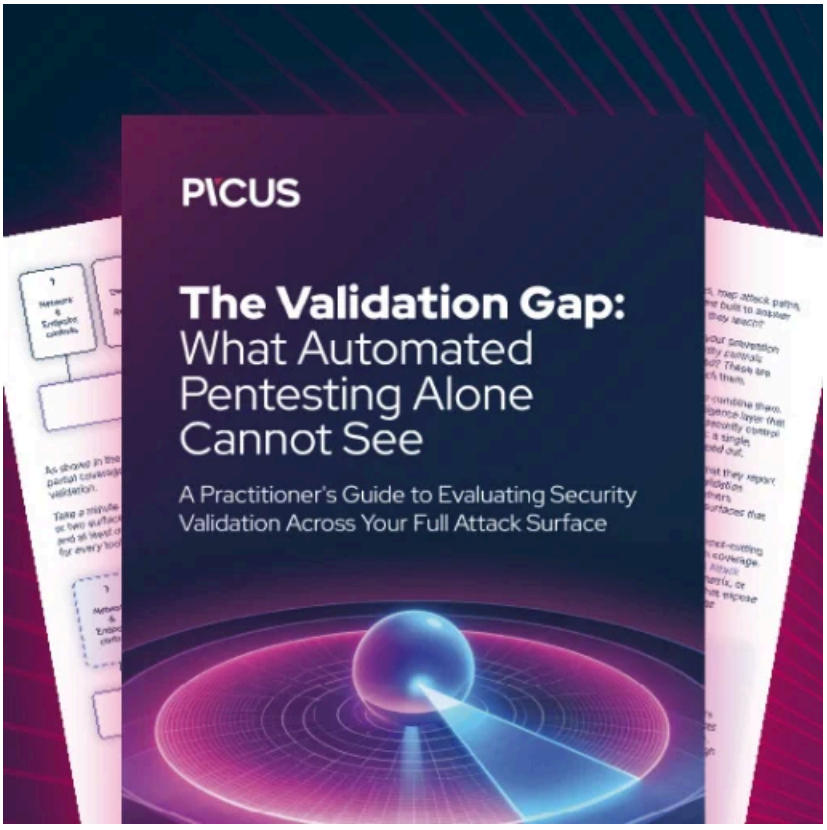
Cisco Talos has also shared technical details about the spyware's infection process and mapped many of its data-theft capabilities.

The inclusion of individuals and entities on OFAC's Specially Designated Nationals (SDN) List has significant legal and financial implications. It is considered a powerful tool in the hands of the U.S. government, used in this case to underline the Biden administration's commitment to countering the misuse of spyware technology.

Inclusion in the SDN List means all U.S.-based assets linked to those persons and entities are frozen, and U.S.-linked individuals and companies are prohibited from engaging in any transactions with them. Those who violate these restrictions can face massive fines and imprisonment.

Also, these sanctions send a powerful signal to the international community, dissuading organizations based in US-allied countries from doing business with sanctioned entities or supporting sanctioned individuals.

This action from the U.S. government comes only days after Recorded Future revealed that despite the recent calls for tighter regulation in the commercial spyware space and the public outcry about Predator's shady deployment cases, the spyware was already spreading to new countries in Asia, Africa, and the Caribbean.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/legal/us-sanctions-predator-spyware-operators-for-spying-on-americans/