US cracks down on spyware vendor Intellexa with more sanctions

By Sergiu Gatlan

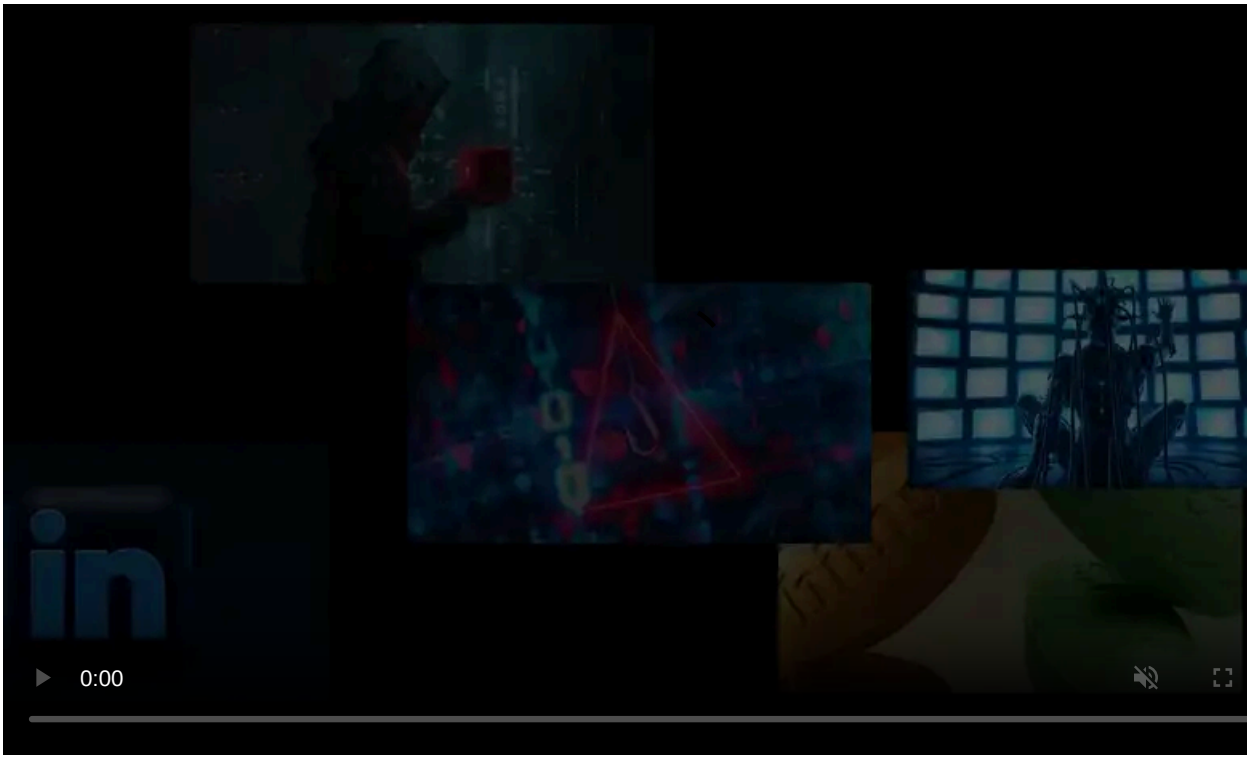
Published: 2024-09-16 · Archived: 2026-04-05 17:00:45 UTC

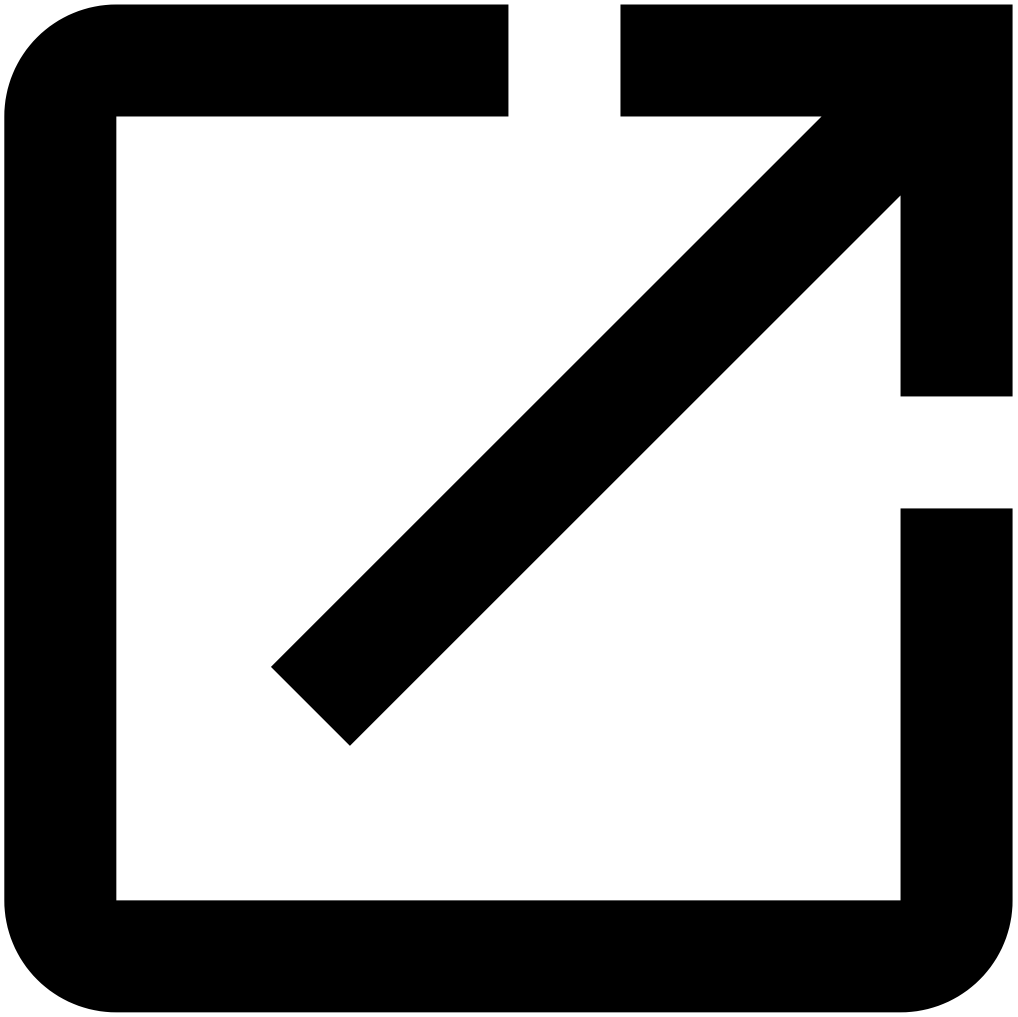
Image: Midjourney

Today, the U.S. Department of the Treasury has sanctioned five executives and one entity linked to the Intellexa Consortium for developing and distributing Predator commercial spyware.

Intellexa Consortium is a network of decentralized companies that developed and sold highly intrusive spyware products marketed under the "Predator" brand.

Predator spyware has allowed Intellexa customers worldwide — mostly state-sponsored actors and governments — to access sensitive information on victims' smartphones, including photos, geolocation data, personal messages, and microphone records in one-click or zero-click attacks.


0:00



Intellexa spyware tools have been used to target government officials, journalists, policy experts, tech executives, and opposition politicians in campaigns to intimidate political adversaries, restrict freedom of speech, suppress dissent, and monitor journalists' activities worldwide and in the United States.

In March, Google subsidiary Mandiant and Google's Threat Analysis Group (TAG) revealed that commercial surveillance vendors have been behind 50% of all zero-day exploits used to target Google products and Android devices in 2023.

New sanctions announced Monday include:

- **Felix Bitzios,** the manager of Intellexa S.A. and the owner of an Intellexa Consortium company that supplied a foreign government client with Predator spyware,
- **Andrea Nicola Constantino Hermes Gambazzi** is the beneficial owner of Thalestris Limited and Intellexa Limited, members of the Intellexa Consortium,
- **Merom Harpaz,** a manager of Intellexa S.A and an Intellexa Consortium top executive,
- **Panagiota Karaol,** the director of multiple Intellexa Consortium entities,
- **Artemis Artemiou,** the general manager and member of the board of Cytrox Holdings (a member of the Intellexa Consortium),
- And **Aliada GroupInc**, a British Virgin Islands company and an Intellexa Consortium member that has enabled tens of millions of dollars of transactions involving the spyware network

"The United States will not tolerate the misuse of technologies that undermine Americans' national security or that of our allies, nor will we tolerate the misuse of technologies to perpetrate human rights abuses or undermine freedom of expression," said State Department spokesperson Matthew Miller.

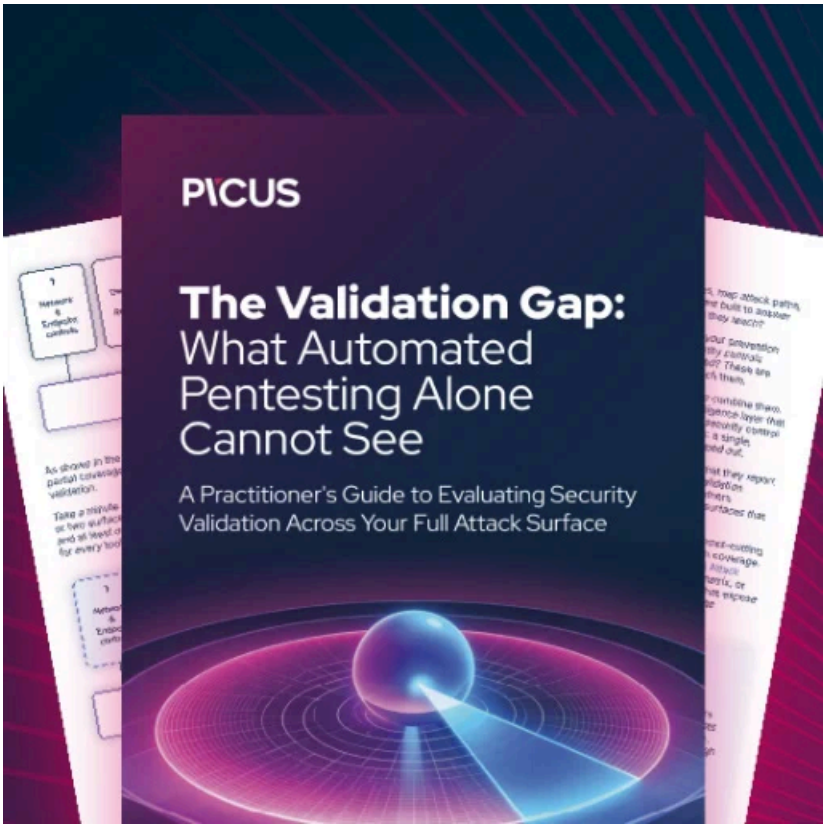
"Today, we are imposing sanctions on five individuals and one entity associated with the Intellexa Consortium for their role in developing, operating, and distributing commercial spyware technology misused to target Americans, including U.S. Government officials, journalists, and policy experts."

This commercial spyware network of entities was founded by Tal Jonathan Dilian (Dilian), sanctioned by the Treasury's Office of Foreign Assets Control (OFAC) in March, together with five entities, including Cytrox AD (North Macedonia), Cytrox Holdings ZRT (Hungary), Intellexa Limited (Ireland), Intellexa S.A. (Greece), and Thalestris Limited (Ireland).

Earlier this year, the State Department announced a new visa restriction policy that would allow banning those linked to commercial spyware from entering the United States, subsequently used to prohibit the entry of 13 individuals linked to commercial spyware operations (and their close families).

In July 2023, the Department of Commerce added Intellexa commercial spyware vendors to its Entity List, citing risks to U.S. national security and foreign policy interests. The U.S. Commerce Department also sanctioned four other companies from Israel, Russia, and Singapore (including Israeli spyware makers NSO Group and Candiru) in November 2021) for their involvement in developing spyware or selling hacking tools used by state-sponsored hacking groups.

Individuals and entities listed on OFAC's Specially Designated Nationals (SDN) List face significant legal and financial consequences. Their inclusion means all U.S.-based assets linked to them are frozen, and U.S.-based individuals and companies are prohibited from engaging in any transactions with them, under the risk of severe penalties and imprisonment.



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/security/us-cracks-down-on-spyware-vendor-intellexa-with-more-sanctions/