

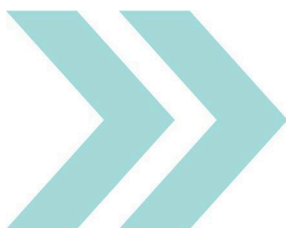
October 8, 2026

To Whom It May Concern at Discover-Tech Ltd.:

The Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, is currently researching your company's products and its uses.

Our research confirms the following:

- We found that mercenary spyware from Candiru (rebranded as "Integrity Labs") was delivered via targeted online advertisements.
- The malicious advertisements were purchased by Discover-Tech Ltd., an Israeli company that presents itself as a legitimate advertising company, but which we found operates as a facilitator for multiple mercenary spyware partners.
- Discover-Tech operates a platform called Controlium that enables its mercenary partners to de-anonymize, fingerprint, and automatically infect devices the moment an advertisement is rendered — a form of zero-click attack that we call **AdFection**.
- Analysis of four billion Discover-Tech bidding records shows that during a three-month period, the company's ads were shown on almost 200,000 unique websites and Android/iOS apps in dozens of countries.
- Discover-Tech's ads also covertly directed millions of devices to contact Candiru's servers, likely for large-scale tracking and reconnaissance. Discover-Tech is linked to mercenary spyware and intelligence threat actors beyond Candiru, including Intelos, and Bindecy.
- A separate threat actor we call **DARK CARTOGRAPHER** is using Discover-Tech's infrastructure to exploit vulnerabilities across numerous mobile carriers to link device advertising IDs with phone numbers, mass-deanonymizing internet users.
- Discover-Tech has appeared on lists of "certified" and "approved" vendors maintained by Google and advertising industry association IAB Europe, and has served ads via major networks such as Google, Yandex, and Beeswax. Discover-Tech has also leveraged GDPR consent frameworks to target users within the European Union.
- Discover-Tech's mass abuse, privacy invasion, and facilitation for mercenary spyware attacks illustrates structural flaws with the online advertising system, which failed to detect or prevent their actions.



munkschool.utoronto.ca

At Trinity College
1 Devonshire Place
Toronto, ON
Canada M5S 3K7
T: 416.946.8900 F: 416.946.8915

At the Observatory
315 Bloor Street West
Toronto, ON
Canada M5S 0A7
T: 416.946.8929 F: 416.946.8877

At the Canadiana Gallery
14 Queen's Park Crescent West
Toronto, ON
Canada M5S 3K9
T: 416.978.5120 F: 416.978.5079

Additional research findings with respect to Discover-Tech Ltd.:

- Our report will also mention an authentication vulnerability in your Controlium app we found on [www.controlium\[.\]net](http://www.controlium[.]net), [powerium\[.\]net](http://powerium[.]net) and other domains. The issue arises because the Controlium app does not use Okta's authenticated token, but instead encrypts user metadata with a static key present in the source code. Thus, anyone who obtains metadata about a valid user of the app could forge a token. We did not exploit this vulnerability as we believe doing so would constitute unauthorized access to Discover Tech's systems.

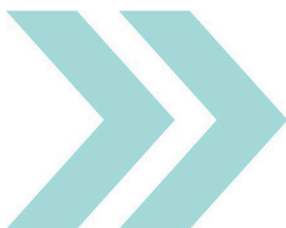
We are seeking a response on our findings described above.

We plan to publish a report reflecting our research. Provided we receive your response by 10 am ET on October 13, 2026, we will publish any response you provide us in full along with our research report. All correspondence with your company will be considered public and included with the final research report.

Sincerely,



Ronald J. Deibert, O.C., O.Ont.
Professor of Political Science
Director, the Citizen Lab at the Munk School of Global Affairs & Public Policy,
University of Toronto



munkschool.utoronto.ca

At Trinity College
1 Devonshire Place
Toronto, ON
Canada M5S 3K7
T: 416.946.8900 F: 416.946.8915

At the Observatory
315 Bloor Street West
Toronto, ON
Canada M5S 0A7
T: 416.946.8929 F: 416.946.8877

At the Canadiana Gallery
14 Queen's Park Crescent West
Toronto, ON
Canada M5S 3K9
T: 416.978.5120 F: 416.978.5079