EXPOSING ADFECTION

How Discover-Tech Turned Targeted Ads Into a Pipeline for Zero-Click Mercenary Spyware



October 15, 2026
Report No. 195

Bill Marczak, Wolfie Christl, John Scott-Railton, Astrid Perry, Siena Anstis, and Ron Deibert

THECITIZENLAB

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

Copyright

© 2026 The Citizen Lab, "Exposing AdFection: How Discover-Tech Turned Targeted Ads Into a Pipeline for Zero-Click Mercenary Spyware," by Bill Marczak, Wolfie Christl, John Scott-Railton, Astrid Perry, Siena Anstis, and Ron Deibert.



Licensed under the Creative Commons BY-SA 4.0 (Attribution-ShareAlike licence). Electronic version first published in 2026 by the Citizen Lab. This work can be accessed through https://citizenlab.ca/research/how-discover-tech-turned-targeted-ads-into-a-pipeline-for-spyware/

Document Version: 1.0

The Creative Commons Attribution-ShareAlike 4.0 license under which this report is licensed lets you freely copy, distribute, remix, transform, and build on it, as long as you:

- give appropriate credit;
- indicate whether you made changes; and
- use and link to the same CC BY-SA 4.0 licence.

However, any rights in excerpts reproduced in this report remain with their respective authors; and any rights in brand and product names and associated logos remain with their respective owners. Uses of these that are protected by copyright or trademark rights require the rightsholder's prior written agreement.

Suggested Citation

Bill Marczak, Wolfie Christl, John Scott-Railton, Astrid Perry, Siena Anstis, and Ron Deibert. "Exposing AdFection: How Discover-Tech Turned Targeted Ads Into a Pipeline for Zero-Click Mercenary Spyware," Citizen Lab Report 195, University of Toronto, October 15, 2026.

Acknowledgements

We thank the teams at Al Jazeera for graciously consenting to our investigating this case, and agreeing to be named in the report.

We thank the teams at Confiant, Google, and additional researchers for their assistance and collaboration in this investigation. We would also like to thank Rebekah Brown, Maia Scott, and Krzysztof Franaszek (Adalytics Research) for peer reviewing this work, as well as other anonymous peer reviewers. Thanks to Adam Senft, Aly Bruce, Anna Mackay, and Claire Posno for editorial and communications support.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is a world-renowned research unit led by Professor Ronald J. Deibert at the University of Toronto's Munk School of Global Affairs & Public Policy. We investigate novel threats to democracy, human rights, and global security in the digital ecosystem. Over the past 25 years, the Citizen Lab's evidence-based research has played a critical role in demonstrating how digital technologies are used to undermine human rights. The Citizen Lab has published more than 180 evidence-based, peer-reviewed research reports, available online.

Contents

Key Findings

1. Introduction
2. How Discover-Tech's AdFection Zero-Click Works
3. Exposing Discover-Tech's Controlium: Malicious Ad Targeting Platform
4. Discover-Tech's Links With Mercenary Spyware, AdInt, and Mass Surveillance Vendors
5. Uncovering Discover-Tech's Billion-Bid Scale Ad Targeting
6. How Discover-Tech Deploys Ads in the Browser
7. Discover-Tech and its Corporate Network
8. Intelos, Bindecy, and Candiru's Corporate Networks
9. Discover-Tech's Relationship to the Digital Advertising Industry
10. Discussion: AdFection Shows That Online Ads Are a Cybersecurity and Privacy Crisis
11. Recommendations: How to Stop AdFection Attacks

Correspondence with Companies

Acknowledgements
Appendix A. Ad Vendors Involved in Discover-Tech's Ad Operations
Appendix B. Glossary
Appendix C. Domains Linked to Discover-Tech and Controlium

Executive Summary

Each time you see a targeted advertisement on a website or in an app, it is usually the result of a winning bid in a split-second digital auction. These auctions, hosted by companies like Google, are designed to help advertisers reach and profile specific consumers. Real-Time Bidding (RTB) auctions process hundreds of billions of bids and ad sales each day. The system broadcasts a vast amount of information about people and their devices that can be used to infer their interests, browsing behaviour, movements, and habits.

This report shows that this ecosystem is being weaponized at a massive scale to profile millions of users, then silently infect targets with zero-click mercenary spyware. We call this type of attack “AdFection.” At the heart of our report is Discover-Tech, an Israel-based mercenary spyware enabler that functions as a link between the exploitable worlds of digital advertising and states undertaking targeted espionage.

This report is the first-ever technical demonstration of in-the-wild infection of devices with zero-click mercenary spyware via targeted advertisements. We find with high confidence that devices at international media network Al Jazeera were targeted and infected with Candiru’s mercenary spyware using AdFection.

This report is co-timed with an investigation by Confiant.

Discover-Tech: A Bridge Between Mercenary Spyware and Online Advertising

Discover-Tech presents itself as a legitimate online advertising business. In fact, the Israel-based company provides a bridge between multiple mercenary spyware companies engaged in hacking and the “legitimate” online advertising ecosystem. Our report found no evidence that Discover-Tech was engaged in legitimate advertising activity.

Discover-Tech’s CEO is Dekel Boni, who has a background in digital advertising. For almost six years, Discover-Tech was associated with principals well known in the mercenary spyware industry. That includes Eric Banoun, who joined the company’s board of directors in 2020 and remained there until 2025. Banoun previously co-founded the surveillance firms Circles and Senpai Technologies, which were closely affiliated with notorious spyware vendors NSO Group and Intellexa. Between 2020 and 2026, Discover-Tech’s shareholders included a company linked to Sara Hamou, who managed the corporate network of Intellexa and was sentenced to eight years in prison (pending appeal) by a Greek court for her role in a spyware abuse scandal in Greece.

Controlium: Zero-Click Targeted Advertising

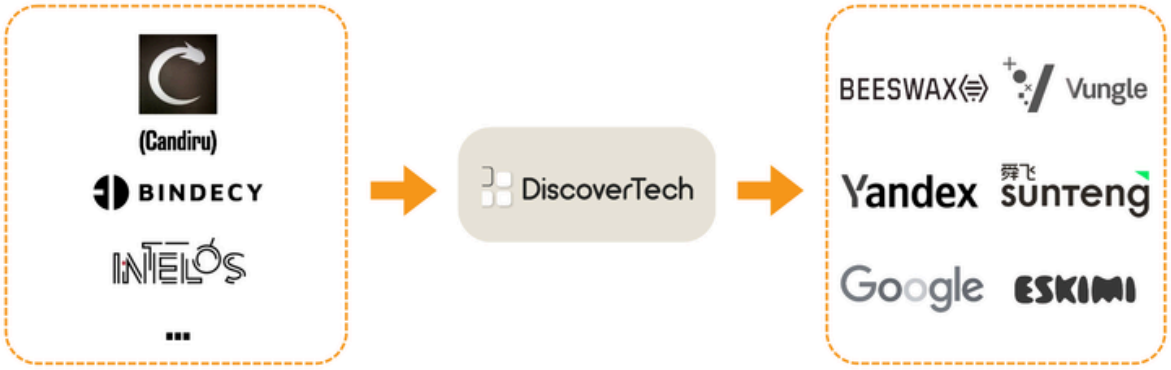
Discover-Tech operates Controlium, a one-stop platform for mercenary spyware firms to infect targets via online ads. Controlium enables these firms to mass-profile and deanonymize millions of users, and

then covertly hack individual targets by sending them seemingly-benign ads containing zero-click exploits to install spyware on their devices.

Controlium's users include mercenary spyware firm Candiru (reportedly now owned by US-based Integrity Labs). Candiru was Entity Listed by the United States Commerce Department for developing spyware used to target "government officials, journalists, businesspeople, activists, academics, and embassy workers." Controlium's platform is also linked to Israel-based Bindecy, which specializes in zero-click mobile exploits, and another mercenary surveillance firm called Intelos.

Profiling and Hacking Ad Recipients

When a user is shown a seemingly-benign targeted ad placed by Discover-Tech, the user's ad identifier and IP address are transmitted to servers operated by Discover-Tech. If the user is selected for hacking, the device is ultimately sent malicious JavaScript code, which is executed by the browser or app. The code then exploits and infects the device.



Discover-Tech bridges the mercenary spyware industry with the online advertising ecosystem.

The fact that the seemingly-benign advertisements do not themselves contain the exploit code helps Discover-Tech conceal the hidden purpose of the ads from the platforms that deliver them.

We have found billions of instances of Discover-Tech bidding to send such advertisements to users, and no sign that the company is engaged in any "legitimate" advertising business activities.

Mass Profiling and Deanonymizing

Discover-Tech interfaces with major global advertising networks including Google, Yandex, and Beeswax, and uses a range of techniques to link a single person across various identifiers and networks, such as IP address and mobile advertising ID.

We analyzed billions of ad bidding records from Discover-Tech and determined the company's advertisements directed millions of devices across dozens of countries to contact their profiling and infection servers.

We observed Discover-Tech ads displayed in apps ranging from DuoLingo to dating apps, period trackers, German weather apps, Yahoo Mail, Viber, and calling apps such as Truecaller.

Discover-Tech appears to favour ads in mobile apps, but we observed a wide range of targeting across websites ranging from popular sites in specific geographies ranging from Armenia and Serbia, to Denmark. We also observed their ads displaying on sites including CBC, AccuWeather, FoxNews, the New York Times, Haaretz, and the BBC, among many others.

Ad Impression Data Highlights Systemic AdFection Risk

Our review of the ad bidding data indicates that Discover-Tech ads were shown on devices in national-security-sensitive networks around the world. These include the networks of various ministries of defense, armed forces, national cyber agencies, intergovernmental organizations and multilateral security organizations including NATO, and networks associated with critical infrastructure. The data also show impressions from the networks of media organizations around the world. At minimum, we assess that these ad impressions would have resulted in profiling by Discover-Tech. In some cases, the impressions could have resulted in code from Candiru or other entities running on the user's device.

A Discover-Tech ad impression does not in and of itself confirm targeting or infection with spyware. However, the fact that Discover-Tech was able to bid on and show ads on these networks highlights the systemic risk posed by AdFection and the advertising ecosystem, and warrants urgent investigation to determine whether any users on these networks were infected with spyware. We also note that our visibility into Discover-Tech's impressions is confined to the data on Discover-Tech's MyDSP platform. This data does not include data from Beeswax and Eskimi, and covers a limited time period. This incompleteness further reinforces the need for follow-up investigation.

NATO and the United Nations

We identified impressions in NATO and United Nations networks.

European Union Entities

In Europe, we identified impressions from the networks of the European Parliament, the European Commission, and the Council of the European Union's General Secretariat.

Nordic Government & Critical Infrastructure Clusters

We identified widespread impressions in Nordic states, including Denmark, Norway and Sweden. We assess that this cluster warrants close scrutiny, and note some of the more concerning findings:

- **In Norway**, Discover-Tech ads were shown to users on the networks of the legislature (Stortinget), the Norwegian Digital Agency (Digitaliseringsdirektoratet), the Norwegian Communications Authority (Nasjonal kommunikasjonsmyndighet), state IT networks (Statens IT), the Norwegian Police (Politiets It-enhet) and serious crime units (Kripos), among many others. Notably, we also identified impressions in multiple county and municipal networks across northern Norway, including near key military installations (e.g. Alta, Harstad, Nordland).
- **In Sweden**, Discover-Tech ads were shown to users on the networks of the Armed Forces, the national grid operator (Svenska Kraftnat), the state owned power company (Vattenfall AB), the national internet exchange (Netnod AB), defense contractor Saab, Volvo Group, university networks including the Chalmers University of Technology, national research funding bodies (Verket for Innovationssystem), and Sweden's national Meteorological and Hydrological Institute (Sveriges Meteorologiska och Hydrologiska Institut).
- **In Denmark**, Discover-Tech ads were shown to users at the national rail network (Banedanmark), the national post (Post Danmark), Denmark's National Research and Education Network (Forskningsnettet), alongside multiple municipal and regional government networks and public health authorities. They were also shown on networks at Denmark's digital infrastructure company KMD A/S, renewable energy sector firms such as Vestas Wind Systems and Ørsted, Grundfos, banks including Den Danske Bank, and Copenhagen Airports.

Australia: Critical Infrastructure, Government & University Networks

The ad impression data also reveal a substantial cluster of impressions in Australia, including on government and private-sector networks associated with critical infrastructure sectors like grid and power companies, as well as networks associated with universities and research centres, including entities working on nuclear research, like the Australian Synchrotron, and the Australian Nuclear Science and Technology Organisation.

Governmental Targets: A Global List

Numerous other geographically distinct clusters of widespread impressions appear among the data. Many of these impressions occurred in defense, foreign affairs, internal affairs, or security bodies. The table below provides examples of the government networks where we found Discover-Tech impressions.

Government	Examples of networks with Discover-Tech impressions
Armenia	Central Electoral Commision Central Bank Office Of The Prime Minister
Czechia	Ministry of Finance Ministry of Foreign Affairs

	Ministry of the Interior State Institute for Drug Control Czech Telecommunication Office Ministry of Agriculture The Czech National Bank Ministry of Labour and Social Affairs Municipal Office, Prague National Cyber and Information Security Agency
Israel	Ministry of Health Ministry of Foreign Affairs Government ICT Authority Ministry Of Defence Israeli Police Bank of Israel Israel Internet Association Israel Airports Authority
Italy	Bank of Italy Parliament (Camera dei deputati) Ministry of Defense

Examples of government controlled or operated networks where we identified Discover-Tech impressions.

Our investigation is ongoing. As of now, we have identified impressions in government-operated networks in the following countries:

- Armenia
- Australia
- Azerbaijan
- Bhutan
- Brazil
- Czechia
- Denmark
- Indonesia
- Israel
- Italy
- Kosovo
- Libya
- Malaysia
- Mexico
- Montenegro
- Norway
- Pakistan

- Russia
- Somalia
- Sweden
- Thailand
- The United Arab Emirates
- The United States (American Samoa)
- Uruguay

We also found impressions on the networks of election oversight bodies in Armenia, Indonesia, and Mexico.

Chips & Semiconductors: From Research to Fabrication

We found what appears to be a nexus among the advanced semiconductor industry, covering the chain from design, memory, to chip development and fabrication, with the greatest number of impressions seen in Intel networks, alongside Nvidia, Sandisk, Texas Instruments, Broadcom, Micron Technology, and ARM. We also identify numerous research entities in this category like IMEC. We also identified impressions within the networks of large U.S. tech firms including Apple, Microsoft, and Motorola.

We also identified impressions in specifically defense-sector tech entities, including Raytheon (U.S.) and Elbit Systems LTD (Israel), and the nuclear sector, including the Westinghouse Electric Company (U.S.).

Global Media Organizations

Given our identification of zero-click attacks against Al Jazeera, we scrutinized bidding records for impressions within the networks of media organizations. We found many. Often, these included the largest media organizations in a particular country, as well as public broadcasters and media conglomerates. The countries (with a count of institutions) include:

- Australia: 3
- Denmark: 3
- France: 1
- Mexico: 2
- Israel: 3
- Italy: 2
- Norway: 2
- Sweden: 3

We also identified impressions within the networks of international media services. Our investigations into these cases are ongoing.

The Digital Advertising Supply Chain: Dangerously Compromised

Our analysis reveals a dangerous lack of due diligence in the advertising ecosystem that Discover-Tech actively exploited. Despite supporting mass-profiling and mercenary spyware hacking, Discover-Tech has nonetheless appeared on several lists of “certified” and “approved” advertising vendors maintained by Google and IAB Europe, the advertising industry association.

The fact that a “certified” company could target millions of users for years with no signs of legitimate activity highlights the dangerously inadequate controls over a sector that by its very nature touches almost every individual with a mobile device or a web browser in extremely invasive ways.

As a result of this investigation, Google and IAB Europe have removed Discover-Tech from their ad vendor lists. Google and Beeswax have terminated the company’s access to their ad systems.

The AdFection attacks and espionage described in this report impact millions of people in dozens of countries. Existing laws and self-regulation by the industry failed to catch or prevent them. Our report provides guidance to regulators, defenders and the advertising industry on how to stop AdFection and ADINT-style espionage.

Excerpt

This is the first-ever public confirmation of zero-click mercenary spyware delivered via targeted ads. We call the technique AdFection, and show how it was used to infect devices at Al Jazeera with Candiru's spyware. We also uncover Discover-Tech, and show how the company helps mercenary surveillance vendors track and hack devices around the world.

This report is co-timed with an investigation by Confiant.

Key Findings

- Devices at international news network Al Jazeera were infected with mercenary spyware from Candiru (rebranded as "Integrity Labs") via targeted online advertisements. We provide the first public technical confirmation of a zero-click mercenary spyware attack delivered via targeted advertising, which we call AdFection.
- The malicious advertisements were purchased by Discover-Tech, 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.
- Analysis of four billion Discover-Tech bidding records shows that during a four-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. We will detail our findings concerning this threat actor in a separate forthcoming report.
- 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 the European General Data Protection Regulation (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 the abuse documented in this report.

- We call on regulators to investigate whether Discover-Tech and Candiru/Integrity Labs violated applicable laws, and make recommendations to lawmakers, defenders, and the advertising industry on how to stop AdFection-style attacks and espionage.
- We disclosed our findings to ad vendors and industry organizations. Google, IAB Europe, Beeswax, Vungle (Liftoff), and Eskimi took action to disconnect Discover-Tech's access to the digital advertising ecosystem. Other ad vendors we found to be involved in Discover-Tech's operations did not respond to our request for comment within the timeline provided. We are also actively working with vendors to mitigate DARK CARTOGRAPHER's mass-deanonymization attack.

Introduction

This section provides an overview of the online advertising ecosystem, and summarizes our findings about Discover-Tech.

The Online Advertising Ecosystem is Ripe for Abuse

When a user sees an ad on an app or a website, it is likely the result of a real-time auction, where advertisers bid on the chance to show that specific user that specific ad. So-called Real-Time Bidding (RTB) auctions, which are hosted on ad exchanges operated by companies including Google, take place hundreds of billions of times a day. In less than a second, the user's device initiates a bid request, advertisers submit their bids, and the ad exchange determines the winner of the auction and pushes the ad to the user. Besides an image or video, an online ad can also contain code that runs within the app or browser that shows the ad.

Both advertisers and publishers of apps and websites use ad vendors that act as their intermediaries in these auctions. Advertisers typically buy ads via a so-called Demand-Side Platform (DSP), and a Supply-Side Platform (SSP) sells ad inventory on websites and apps.

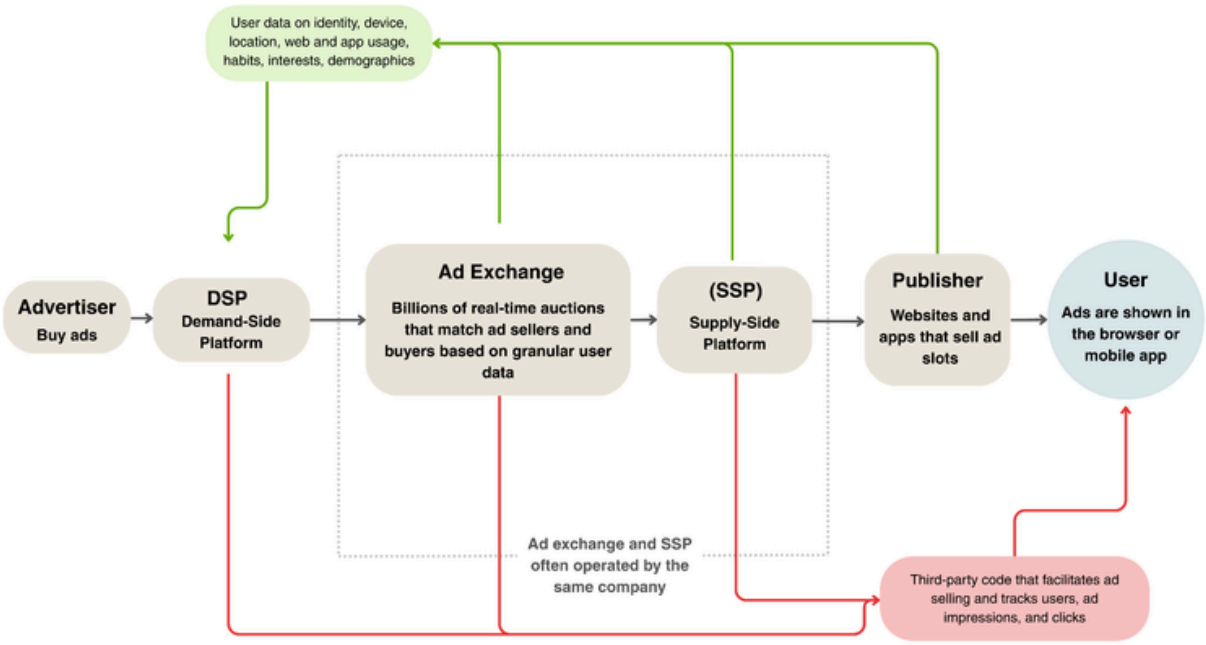


Figure 1: Basic architecture of the online advertising ecosystem.

Malicious actors make use of two interrelated facets of the online advertising ecosystem:

The advertising ecosystem collects a lot of data and enables individual-level targeting: When a publisher of an app or website wishes to show ads, they add code from an SSP to their app or site. This code collects and shares granular information about the user and their device with ad exchanges to solicit bids for the ad slots. This information can include device identifiers and characteristics, precise location, and IP address data, as well as data about the app or website, and specifications about the ad slot. The DSP or advertiser then examines this information and decides whether they wish to bid on the impression in order to show an ad. The auction system is designed to enable targeting single individuals based on their mobile advertising ID, cookie ID, IP address, and other identifiers.

The advertising ecosystem allows many different third parties to run code in apps and websites: It is tempting to think of an online ad as, simply, a video or image. However, ads themselves may contain code from the advertiser, DSP, and other parties, and run it in the app or browser while the ad is shown to the user, for example to track users, ad impressions, and clicks. Code run by advertisers, DSPs, SSPs, and other third parties within apps and websites is often referred to as “tags”, “pixels”, “SDKs”, or “third-party tracking” more generally.

Exploiting Advertising Tech for Surveillance

The totality of information gleaned from ad auctions is quite valuable. A company with access to auction data can track users without their knowledge as they move around in physical space, or switch between cellular, Wi-Fi, and VPNs, by observing how bid requests tied to a specific identifier change location or IP address over time. In fact, the surveillance industry sells access to so-called ad intelligence (ADINT) platforms that leverage this sort of data, often combined with third-party tracking data. In recent years, several investigations and media reports have uncovered vendors that sell ADINT to defense, intelligence, and law enforcement agencies.

Zero-Click Spyware Delivered via Targeted Ads: AdFection

Beyond passive data harvesting, malicious parties can also exploit this infrastructure to target certain individuals based on user data included in ad auctions and then run malicious code on their devices. Advertisers or DSPs may run HTML and JavaScript code when an ad is shown to the user. That code retrieves additional JavaScript code, which may, in turn, load further code, such as a browser exploit to install spyware. Since the code can contain identifiers for the user or their device, arbitrary JavaScript code can be sent precisely to a single user's device. Our research in this report indicates that this architecture is indeed abused to facilitate the delivery of zero-click targeted spyware, and that the simple display of a targeted ad is enough for infection.

There has been some reporting about the intersection between spyware and the advertising ecosystem. However, the specific ways mercenary spyware companies plug into the ads ecosystem to target particular users have remained largely secret. **This report exposes zero-click spyware delivered via targeted ads, which we call AdFection, and is the first technical demonstration that mercenary spyware is being distributed via targeted advertisements.**

Discover-Tech is a Bridge Between Mercenary Spyware Companies and the Advertising Ecosystem

We present technical evidence that the Israel-based company Discover-Tech, while purporting to be a legitimate advertising company, appears to be a front for large-scale ad espionage abuse, including the automatic delivery of mercenary spyware when ads are displayed to a target and the mass profiling and deanonymization of users.

The company serves as a bridge between ad vendors and the mercenary spyware ecosystem. In fact, it appears that serving as this bridge is Discover-Tech's primary purpose. Its platform, Controlium, allows malicious actors to precisely profile and de-anonymize millions of individuals, fingerprint their devices, and target them with a form of zero-click hacking, where their devices can be automatically infected when an ad is displayed to them.



Figure 2: The website of Integrity Labs (the rebranded Candiru), one of the mercenary spyware companies working with Discover-Tech.

Discover-Tech appears to work with multiple mercenary spyware, hacking, and advertising vendors, connecting the spyware industry to the online advertising ecosystem. As we detail in this report, Discover-Tech ads are used to infect and profile on behalf of mercenary spyware vendor Candiru. We also detail connections between Discover-Tech and another mercenary hacking company, Bindecy, as well as connections with Intelos, a mercenary ADINT firm.

What is Discover-Tech and How Does It Operate?

Discover-Tech is led by its CEO Dekel Boni, who has a background in digital advertising. Eric Banoun, whom Haaretz describes as "one of the pioneers of offensive cyber in Israel", joined the company's board of directors soon after it was founded in 2020 and remained there until 2025. Between 2020 and March 2026, Discover-Tech's shareholders included a company linked to Sara Hamou, who has managed the corporate network of the spyware group Intellexa.

Discover-Tech appears to place advertisements using several techniques. Firstly, the company operates a platform called **MyDSP**, which interfaces with online ad vendors including Google, Yandex, Vungle (Liftoff), and Sunteng. Secondly, separately from MyDSP, it purchases ads via the ad vendors Eskimi and Comcast-owned Beeswax (Freewheel).

A large number of ads placed by Discover-Tech contain a script tag pointing back to what the company refers to as a "**NOAS server**" (also called a "getAd server"). This tag causes the ad, when rendered, to connect back to Discover-Tech, submit advertising identifiers for the user (either a cookie ID or a mobile ad ID), and automatically execute any JavaScript code returned. The NOAS server decides, apparently based on a combination of the source IP address and the advertising identifiers, whether the target is eligible to receive any JavaScript. If so, then code is returned. If not, a 0-byte response is returned. The NOAS server is a key part of Discover-Tech's strategy, allowing Discover-Tech to avoid directly sharing malicious code, or even pointers to malicious code, with the companies who serve and display the ads.

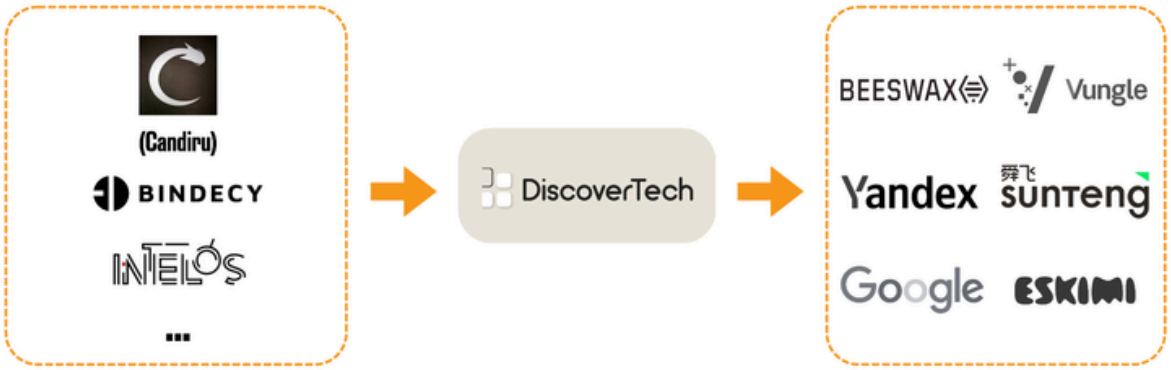


Figure 3: Discover-Tech bridges the mercenary spyware industry with the online advertising ecosystem.

As detailed in Section 9, Discover-Tech appeared on several lists of "certified" and "approved" ad vendors maintained by Google and the advertising industry association IAB Europe from the year 2020 until 2026. These listings helped make Discover-Tech appear to be a legitimate ad vendor and facilitate its participation in the digital advertising ecosystem at scale.

As a result of this investigation, both Google and IAB Europe removed Discover-Tech from their ad vendor registries in early October 2026. Google, which collaborated in the investigation, terminated Discover-Tech's access to its ad exchange platforms. Beeswax removed Discover-Tech from its ad buying platform, Vungle (Liftoff) paused Discover-Tech's access while conducting a review, and Eskimi blocked Discover-Tech's accounts and domains.

Report Overview: Exposing Discover-Tech's AdFection Pipeline

In this report we provide an overview of the different types of ad abuse facilitated by Discover-Tech, the company's ad targeting systems and practices, as well as its partners and corporate network.

In **Section 2**, we show how Candiru works with Discover-Tech to conduct AdFection attacks, and describe one such attack: the targeting and infection of devices at the international media network Al Jazeera with Candiru's mercenary spyware.

In **Section 3**, we examine Controlium, a Discover-Tech platform that provides a control-panel style interface enabling mercenary spyware customers to target specific users with "controlled ads."

In **Section 4**, we examine links between Discover-Tech and mercenary spyware companies Candiru/Integrity Labs and Bindecy. We then outline their relationships with other mercenary surveillance companies, including advertising intelligence (ADINT) vendor Intelos, and an ADINT vendor we refer to as ***DARK CARTOGRAPHER***, which is building databases linking users' mobile advertising identifiers to their phone numbers.

In **Section 5**, we analyze *where* Discover-Tech's malicious advertisements land. We identified a Discover-Tech server that published almost four billion ad bidding records. These records show that Discover-Tech ads were served in almost 200,000 different Android apps, iOS apps, and websites in many countries. We also highlight specific countries and government networks where Discover-Tech's advertisements had impressions.

In **Section 6**, we use technical analysis to examine how Discover-Tech deploys ads, tracks users and exchanges user identifiers with other ad vendors, including with Beeswax, Yandex, and Microsoft's ad system Xandr.

In **Section 7**, we present our research on Discover-Tech Ltd, its corporate network, key persons linked to the company, the origins of its MyDSP advertising technology, and its connection to the wider advertising ecosystem.

In **Section 8**, we summarize what is known about the mercenary surveillance firms Candiru, Bindecy, and Intelos, and we further examine their activities and corporate networks in the context of the findings presented in our report.

In **Section 9**, we explore how major industry organizations and ad vendors helped enable Discover-Tech's ad operations, including Google, IAB Europe, Beeswax (FreeWheel/Comcast), Vungle (Liftoff), Eskimi, Sunteng, and Xandr (Microsoft).

In **Section 10**, we discuss the implications of AdFection for user security and human rights.

In **Section 11**, we provide recommendations to lawmakers, regulators, defenders, and the advertising industry on how to mitigate and block threats from AdFection-style attacks.

The Citizen Lab sent requests for comment to 13 companies; their responses are included in full in the 'Correspondence with Companies' section.

2. How Discover-Tech's AdFection Zero-Click Works

This section provides the first public technical confirmation of a zero-click spyware attack via targeted ads in the wild: the targeting and infection of devices at the international media network Al Jazeera with mercenary spyware. We refer to this type of attack as ***AdFection****. Using network analysis, infrastructure fingerprinting, and analysis of implant behaviour, we connect Discover-Tech's infrastructure with the distribution of Candiru's mercenary spyware.*

What AdFection Looks Like

The instances of Candiru AdFection via Discover-Tech ads all share similar characteristics. First, Discover-Tech wins a bid, and one of their ads is pushed to a website or app that is open on a user's device. The user may see this ad, such as in **Figure 4**, though in some cases the ad may render in the background.

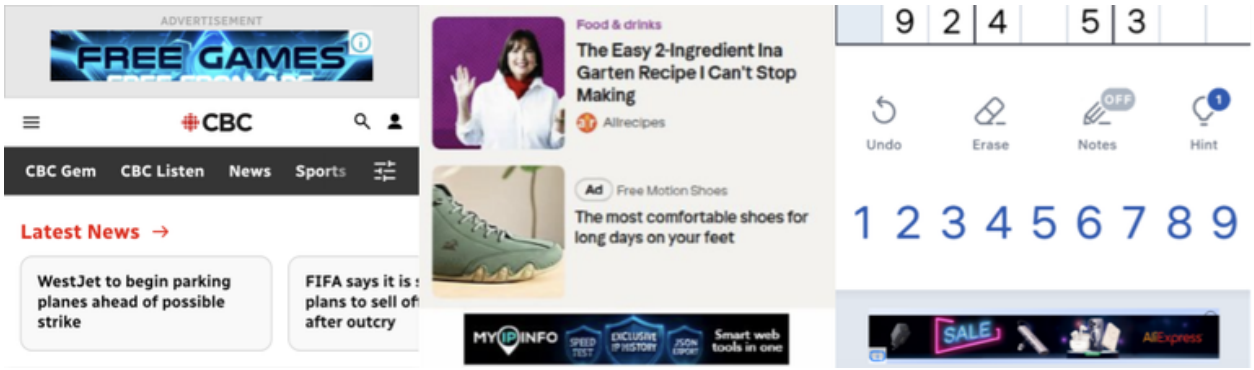


Figure 4: Discover-Tech ads that could have infected users with spyware. We were served these ads while browsing the CBC and Yahoo websites, and while using a Sudoku app on Android.

When the website or app receives the ad, it renders it, requesting JavaScript from a Discover-Tech server embedded within the ad. In most cases, the user who sees the ad is *not* selected for targeting, and the server will *not return any* JavaScript to be executed. Nevertheless, the ad will still gather data from the user's browser and submit it back to Discover-Tech, which can include cookies set on the webpage including the ad, as well as the device's public IPv6 address.

Confirming the Targeting of Al Jazeera with Candiru Spyware via Discover-Tech Ads

In 2024 and 2025, international news network *Al Jazeera* was targeted in a series of zero-click attacks that we link with high confidence to Candiru's spyware delivered via Discover-Tech's ads. At least 45 devices within Al Jazeera were targeted in these attacks.

Analysis of network logs provided to the Citizen Lab by Al Jazeera collected during the attack period provides a clear temporal signature of how the attack was executed. Infected devices first show contact with domains from Discover-Tech infrastructure, indicating an ad impression. Next, the devices show connections with a Candiru validator server. The validator server performs an initial check of the device before it is further profiled and infected. Ultimately, an infected device communicates with a Candiru Command and Control (C&C) server. This temporal signature is illustrated by **Figure 5**.

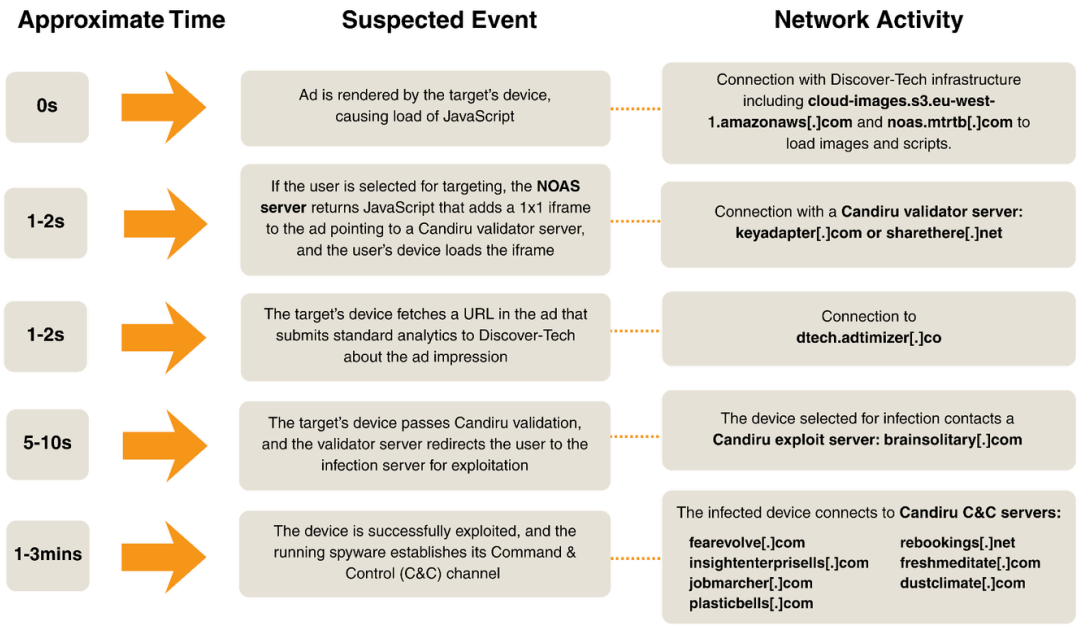


Figure 5: Temporal signature of a Discover-Tech facilitated Candiru infection.

Fingerprinting Candiru Servers

We developed a fingerprint for Candiru validator servers. Both `keyadapter[.]com` and `sharethere[.]net` returned banners that matched the following regular expression on Censys.[1] We

[1] Note that the "\r?" after the date header is due to a 2022 Censys bug and does not relate to server behaviour. Anyone seeking to write signatures over HTTP banners on Censys, who wishes those signatures to be applicable to the 2022 timeframe, should make a similar modification to their signatures.

refer to this as **Fingerprint V1**:

```
HTTP/1\.1 [^\r\n]+\r\ndate: [^\r\n]+\r?\n(connection:
[^\r\n]+\r\n)?content-type: [^\r\n]+\r\nserver:
Apache[^\r\n]*\r\ncontent-length: [0-9]+\r\n.*
```

We found hosts on Censys matching **Fingerprint V1** between August 2022 through July 2026, though we note that in May and June 2026, this behaviour gradually began being retired. In all, we found 305 distinct domain names on 319 IP addresses, though to save query costs we only searched one historical Censys snapshot per month. The set of 305 validator server domains we found includes ones publicly attributed to Candiru by Sekoia, as well as Recorded Future.

We also identified a separate fingerprint for the C&C servers used in the attack, **Fingerprint C1**. Four of the servers matched it (`fearevolve[.]com`, `insightenterprisells[.]com`, `jobmarcher[.]com`, `plasticbells[.]com`). We could not locate a response in Internet scanning data for the other three.

```
HTTP/1\.1 [0-9]+ \r\nDate: [^\r\n]+\r?\nContent-Type:
text/html[^\r\n]*\r\nContent-Length: [0-9]+\r\nConnection:
keep-alive\r\nserver: nginx\r\n$
```

Attribution of the Attack to Candiru

Al Jazeera isolated a Windows DLL file from one of the compromised devices which contains hardcoded Command & Control servers matching Fingerprint C1. The sample is available on VirusTotal.

Candiru spyware sample SHA256:
255869de85e2a171993fc5eb8a556d873a1b8966e040f6f55926f2fa2d595cc8

This sample hard-codes two C&C servers that match **Fingerprint C1**: `fearevolve[.]com` and `jobmarcher[.]com`. The functionality broadly overlaps with the functionality of the Candiru chain from our 2021 report. For example:

- Both samples use a COM hijack for persistence, though make use of different DLLs.
- Both samples obfuscate strings using a 48-byte repeating XOR key, though the samples have different keys. Both samples also have an interesting quirk where obfuscated strings contain a “dummy” null-terminator character that is not deobfuscated (the deobfuscation with the key would be nonsensical), and is instead silently discarded. The only function of this dummy null-terminator appears to be to ensure that the right-size chunk of memory is allocated to hold the XOR-decrypted output.

- The configuration within both samples hardcodes the same ordered list of domain names to fetch to check network connectivity: `http://www.google.com` and `http://www.microsoft.com`.

The combination of the COM persistence hijack, the use of a distinctive 48-byte repeating XOR obfuscation technique with a "dummy" null terminator, and the specific hardcoded network connectivity check leads us to conclude with high confidence that this sample is a newer version of the Candiru attack chain that we captured in 2021.

3. Exposing Discover-Tech's Controlium: Malicious Ad Targeting Platform

This section examines Controlium, a platform that provides a control-panel style interface allowing mercenary spyware customers to target specific users with "controlled ads" that deliver malware. Discover-Tech published the full source code for Controlium's frontend on the app's login page, which allowed us to review and reconstruct the user interface.

Discover-Tech provides its customers with access to a platform called **Controlium** that appears to be specifically designed to allow them to push malicious content to individual targeted users alongside advertisements. Customers can use Controlium to select a user for infection or profiling based on their mobile advertising identifier (iOS or Android), browser identifier (MyDSP or Beeswax cookie ID), and/or IP address. Discover-Tech's malicious ads (referred to as "controlled ads") sometimes also contain branding of companies that are closely linked to Discover-Tech, or branding from apparently unwitting third-party companies, including Amazon and AliExpress. We have no evidence that these ads were purchased by Amazon or AliExpress.

As is standard for many web apps, the entirety of the source code for the Controlium frontend is included on the app's login page. We visited the login page in a web browser and saved the page to disk to obtain a copy of the frontend.[2] We modified our copy of the code to remove any communication with any external servers, and to reveal all available screens in the UI. We then opened this version in a web browser to explore the app's user interface.

In our analysis of Controlium, we downloaded only publicly accessible resources without circumventing any access controls. Most data associated with Controlium, such as information about Discover-Tech's customers and their operations, is intentionally protected with an authorization token. However, we were able to obtain data on Controlium user logins from an unauthenticated API endpoint (see below: 'Unauthenticated Endpoint'). We also assess that it would have been possible for a hacker to spoof a valid authorization (see below: 'Authentication Vulnerability'), although we did not test this.

[2] We also submitted several of the bundle.js files containing the frontend to the Internet Archive's Wayback Machine (1, 2, 3, 4) to assist in future investigations by other researchers.

Attribution to Discover-Tech

We found the Controlium platform available on the following websites:

```
www.controlium[.]net
powerium[.]net
adv45.volasim[.]com
adv50.volasim[.]com
```

These domain names all had CNAME records pointing to an AWS Application Load Balancer (ALB) with the name:

```
discovertech-alb-100966113.us-east-1.elb.amazonaws[.]com
```

Additionally, several strings in the Controlium code directly reference Discover-Tech:

```
controlium-discover-tech
https://discovertech.us.auth0.com
```

Furthermore, if a user tries to access a particular endpoint in the app called "/jsConfig", the app displays the following message, which is a possible reference to Discover-Tech's CEO Dekel Boni:

```
message = 'ONLY DEKEL IS ALLOWED!!!';
```

Finally, an unauthenticated API endpoint (see below: 'Unauthenticated Endpoint') shows frequent login activity from users whose names overlap with Discover-Tech employees on LinkedIn.

Controlium: Examining Admin Mode

An account designated as an "admin" on the Controlium platform can configure a number of different parameters for customers of the platform. First, an admin may grant a customer access to the web interface, or the API. It also appears that the Controlium product can be "white labeled" with a different logo, and that access can be restricted to specific IPs.

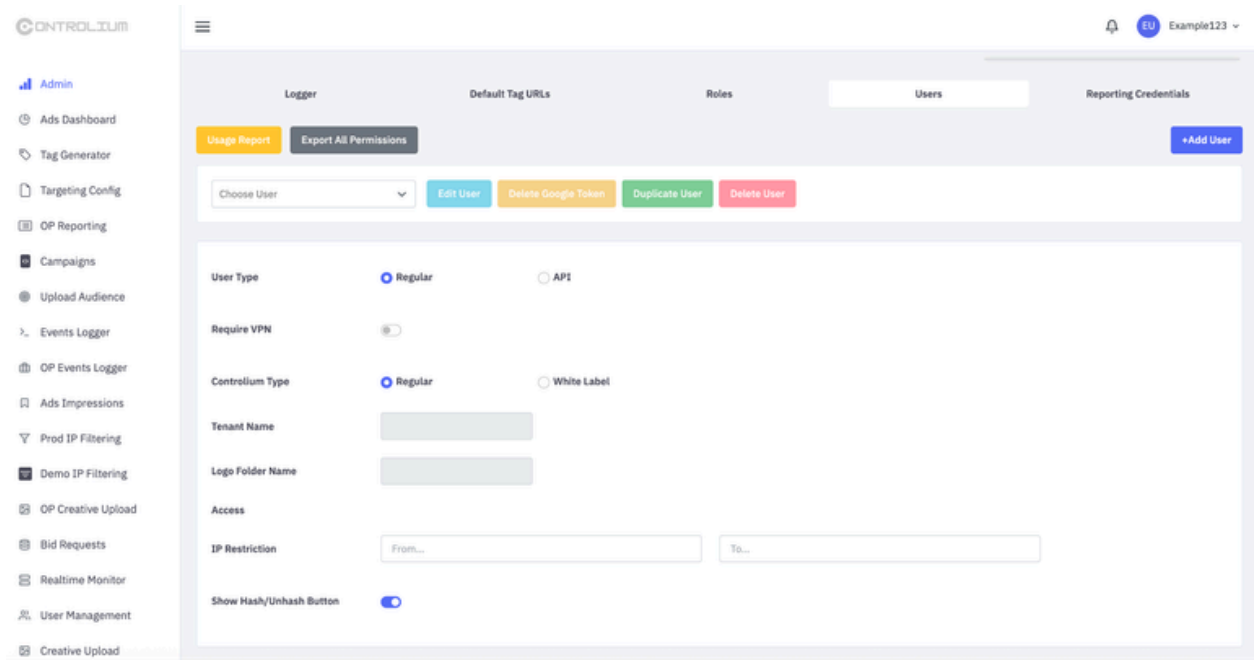


Figure 6: The user admin interface of Controlium

Next, admins may add restrictions on what type of campaigns a customer may run. These restrictions control which combinations of user IDs and IP addresses they are allowed to bid on, and which “URL Types” they can access.

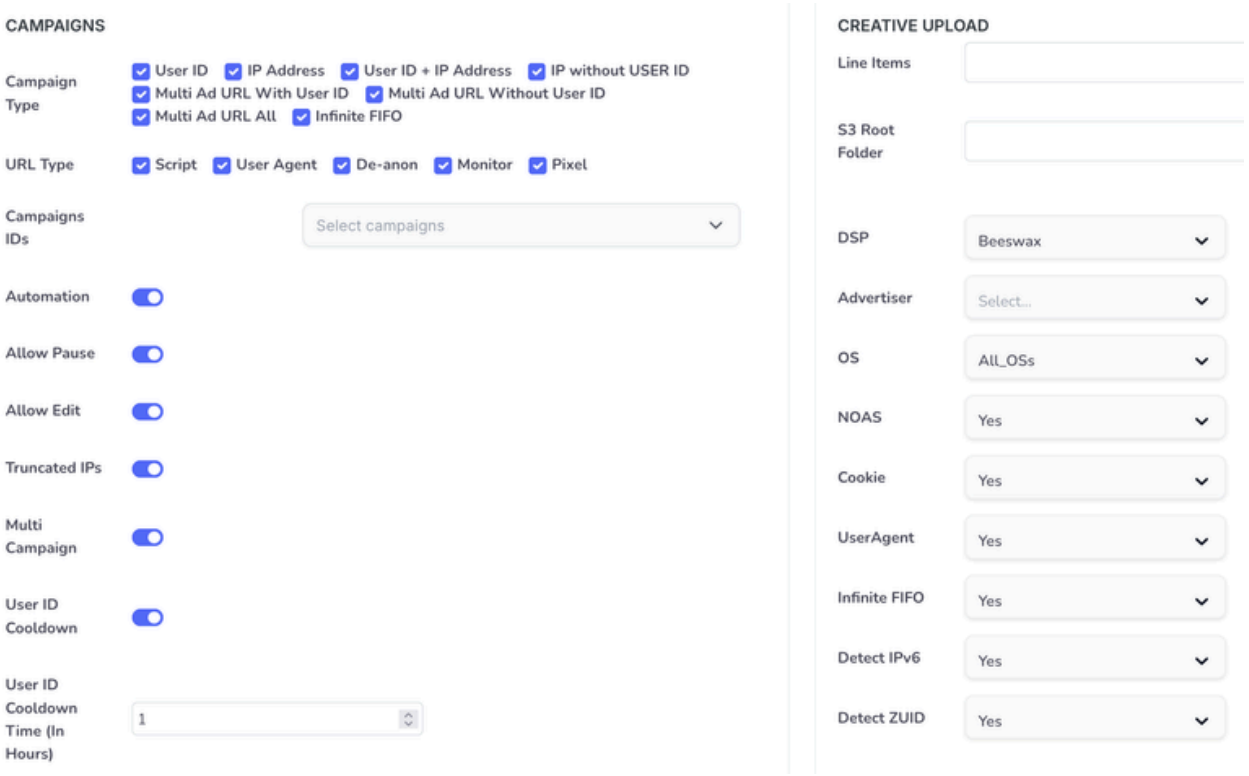


Figure 7: Screenshot of Controlium's admin interface with all options checked.

Customers can have certain "OpSec" restrictions placed on their ad bidding, which appears to be an effort to ensure that customers are not bidding too frequently or too broadly:

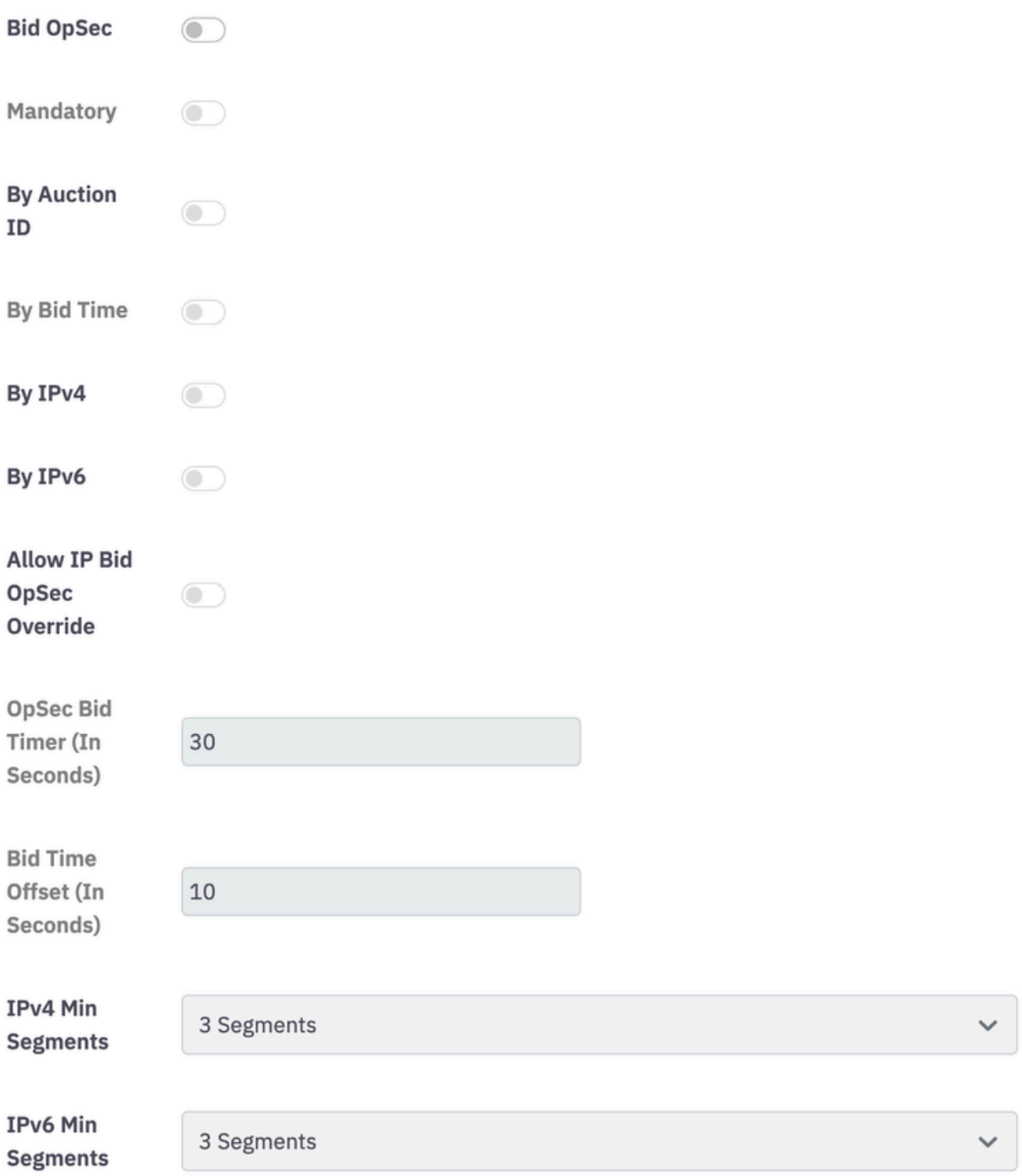


Figure 8: Screenshot of Controlium's admin interface.

There is also another type of "OpSec" called "Ad URL OpSec", which we explore more in Section 4.

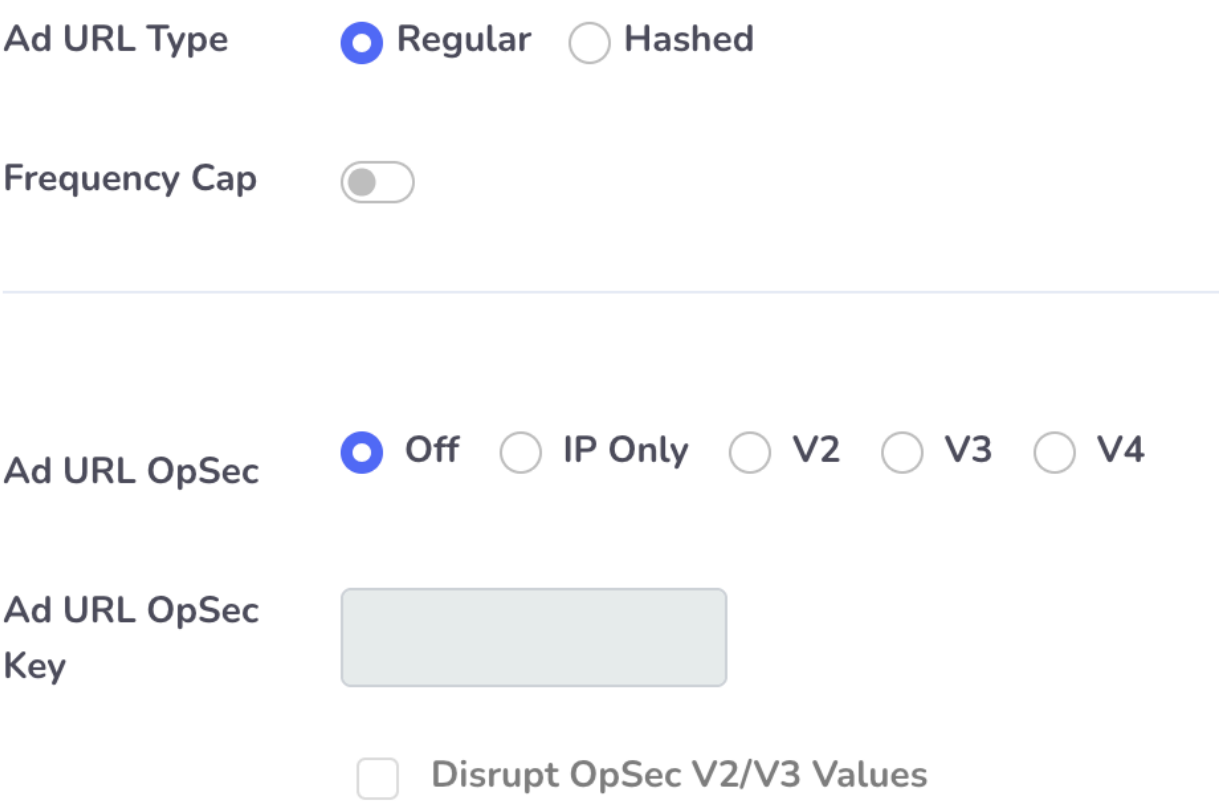


Figure 9: Screenshot of Controlium's admin interface.

Customers can be further restricted based on how many campaigns they can run daily or monthly, or restricted based on a "Domains Whitelist" or "Apps Whitelist", which appear to control on which domain or within which mobile apps ads can be bid on. As is customary for licensing of an attack platform, customers can be restricted to only bid on ads in certain countries via either an allowlist or blocklist.

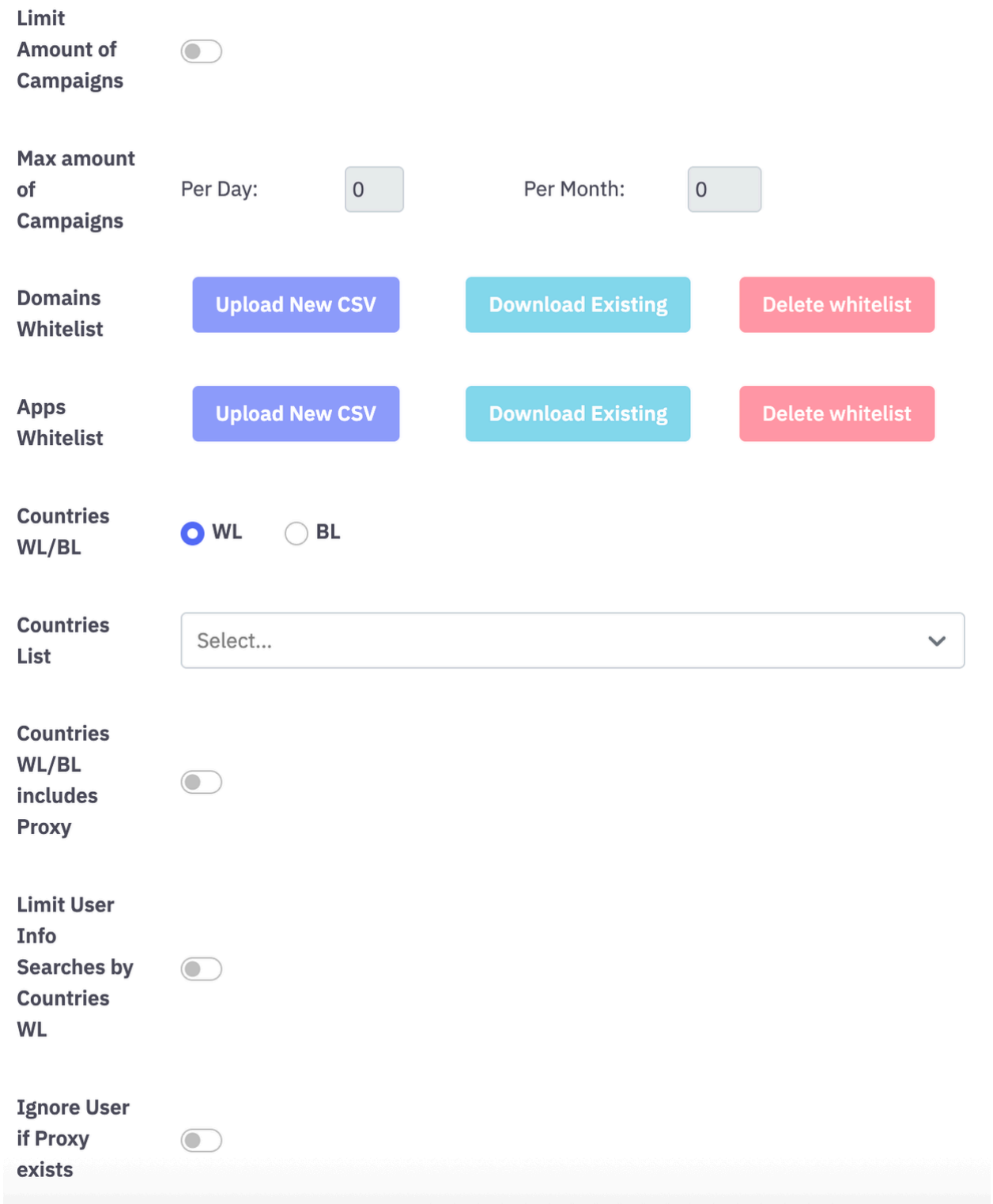


Figure 10: Screenshot of Controlium's admin interface.

Controlium: Examining Customer Mode

The exact steps a user or customer would need to take to use the platform are not clear. The Controlium user interface includes a number of modules and forms that provide, in part, overlapping functionality to set up ad campaigns and monitor ad data.

Controlium users can create a "tag", which defines a combination of an ad image, a landing page, a "NOAS URL" (see below: 'A Look at the NOAS Server'), and URLs for logging impressions and clicks.

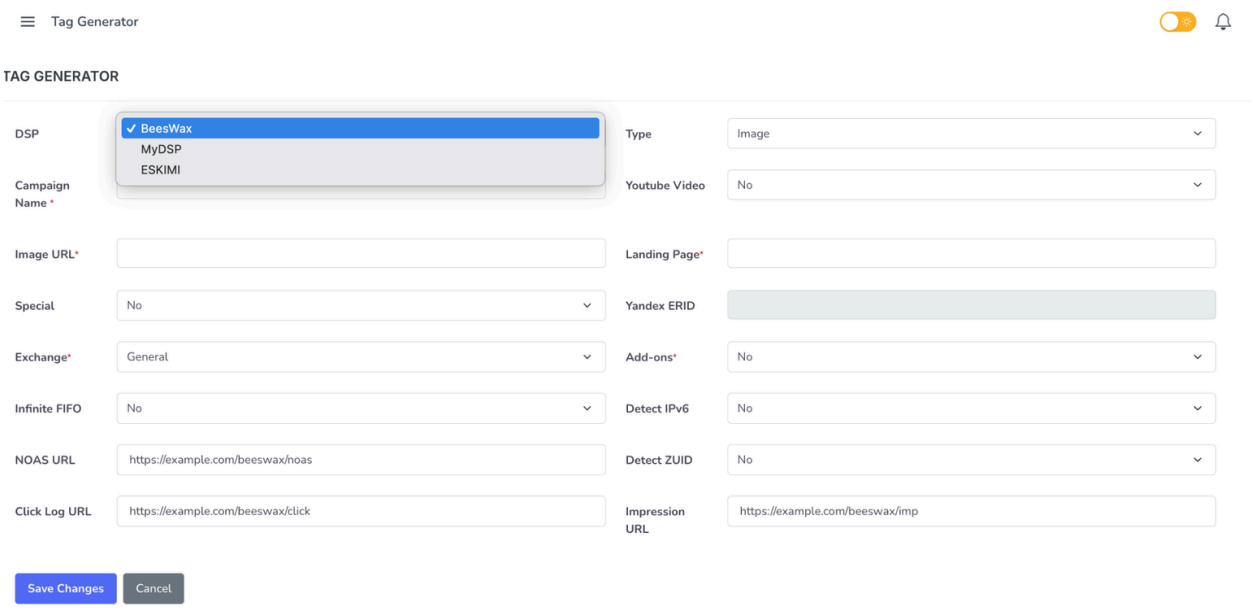


Figure 11: Screenshot of Controlium's Tag Generator module.

Users can select a DSP to use for delivering the ad. The available options include Beeswax, Eskimi and Discover-Tech's own MyDSP. When selecting MyDSP, they can also choose whether to use the Google or Yandex ad exchange.

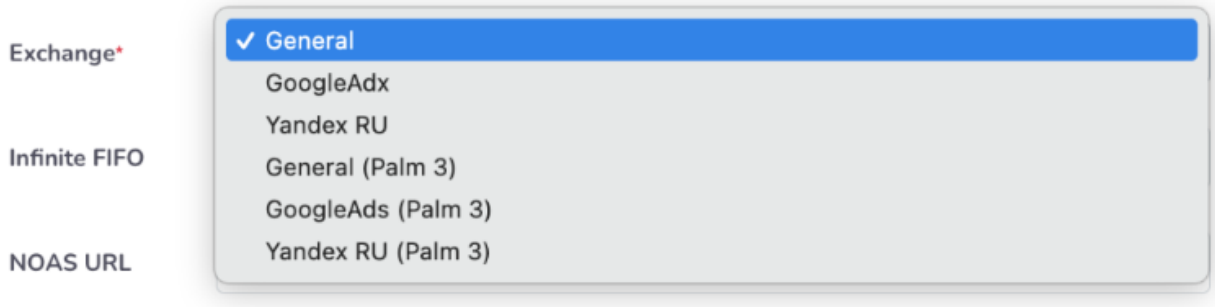


Figure 12: Screenshot of Controlium's Tag Generator module.

Controlium's "OP Creative Upload" module allows users to upload and configure advertising content (e.g. an ad), and then upload the data to a DSP. Users can attach a tag to the ad either by defining a landing page, a NOAS URL and URLs for logging impressions and clicks, or they can paste a "Custom Tag" generated by the "Tag Generation" module.

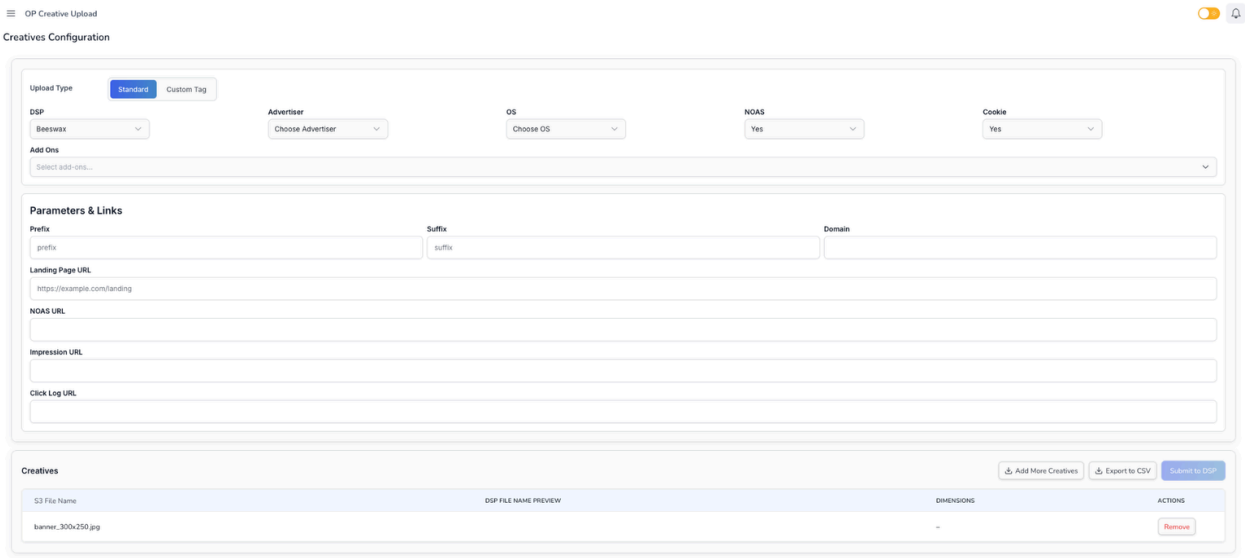


Figure 13: Screenshot of Controlium's "OP Creative Upload" module.

The available DSP options include "MyDSP WW", "MyDSP Yandex RU", "Beeswax (Palm 3)", "MyDSP Google (Palm 3)", and others. Users can also select several "Add Ons" including "Infinite FIFO", "Detect Zuid", and "User Agent".

Another module labeled "Campaigns" allows Controlium users to associate "Ad URLs" to selected "controlled ads", which can be served either in mobile apps or on websites, according to Controlium's source code. As shown in the screenshot, the module allows users to define target "User IDs" and select a "URL Type".

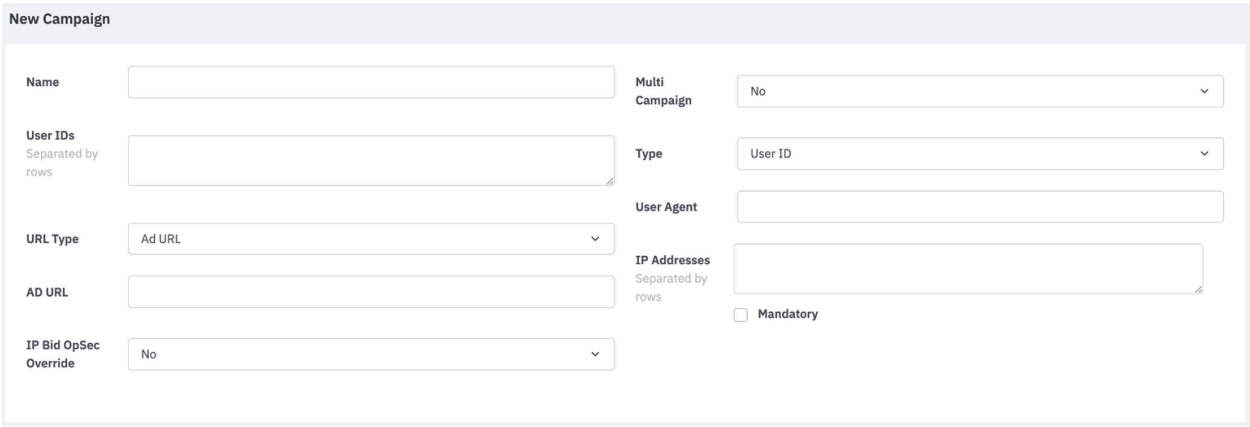


Figure 14: Screenshot of Controlium's "Campaign" module.

The URL types available for selection include "Ad URL", "Test URL", "Script", "User Agent", "Monitor", "Pixel", and "De-anon". We are unsure what most of these options mean, but we think that for "Ad URL", the NOAS server returns JavaScript adding a 1×1 iframe to the page pointing at the specified URL, and "Script" may be designed to allow arbitrary JavaScript to run. Any URL is delivered via the NOAS Server (see below: 'A Look at the NOAS Server').

Authentication Vulnerability

While the data associated with Controlium's customers and their operations are nominally protected with an authorization token, it appears that it would be easy for a hacker to spoof a valid token. We did not attempt to exploit this issue, as we believe doing so would have constituted unauthorized access to Discover-Tech's systems.

```
// const getToken = async () => {
//     if (isAuthenticated) {
//         const token = await getAccessTokenSilently();
//         // localStorage.setItem('token', token);
//     }
// }

useEffect(() => {
    if (isAuthenticated && user) {
        dispatch(LoginAction(user, false));
        // Encrypt
        var ciphertext = CryptoJS.AES.encrypt(JSON.stringify(user), CRYPTO_SECRATE_KEY).toString();
        localStorage.setItem('token', ciphertext);
    }
}, [isAuthenticated, user, dispatch]);
```

Figure 15: Controlium incorrectly derives the authentication token from encrypted user metadata, instead of the signed JWT returned by Okta.

The underlying issue stems from Discover-Tech's improper use of Okta's *Auth0* product. When a Controlium customer authenticates with *Auth0*, a JWT is returned to their browser. This token is digitally signed by *Auth0*, and contains information about scopes and expiry that the backend server should validate. However, Controlium ignores this token and instead passes a separate *user* object as a token to the backend server. The *user* object simply contains unauthenticated metadata about the user, such as their name and email address. Controlium encrypts this information with a secret key published in the Controlium platform.

Interestingly, the *correct* code to use the JWT as an authorization token was present within the Controlium platform, but was commented out in lieu of the vulnerable code.

Unauthenticated Endpoint

During our analysis of the Controlium platform, we observed that the source code mentioned an endpoint called "/csv-download", which accepted start and end date parameters. When we sent normal HTTP GET requests to this endpoint without any password, special headers, or authentication token, we received logs showing which users had logged in to Controlium, and from which IP addresses. We successfully exported authentication logs for 128 days and identified 120 distinct usernames logging into the Controlium instances on `controlium[.]net` and `powerium[.]net`. We further delve into this data in Section 4.

A Look at the NOAS Server

We were able to elicit code from NOAS servers by testing "dummy" User ID values. For example, we observed that a visit to:

```
https://pqv2.mtrtb[.]com/getAd?idfa=test2
```

Yielded the following content:

```
var ifrm = document.createElement("iframe"); ifrm.setAttribute("src",
"https://logger.powerium.net/register_event?user=dbdt&user_id=test2&bundle=
&domain=&user_sha1=&exc=&name=test2&bt=&ai=&referer=&devicemodel=");
ifrm.style="width:1px; height:1px; border:none;";
document.body.appendChild(ifrm);
```

We also found that we could task a NOAS server for a similar Discover-Tech app published on events-ui.myweb3id[.]io called "Mini Platform C".

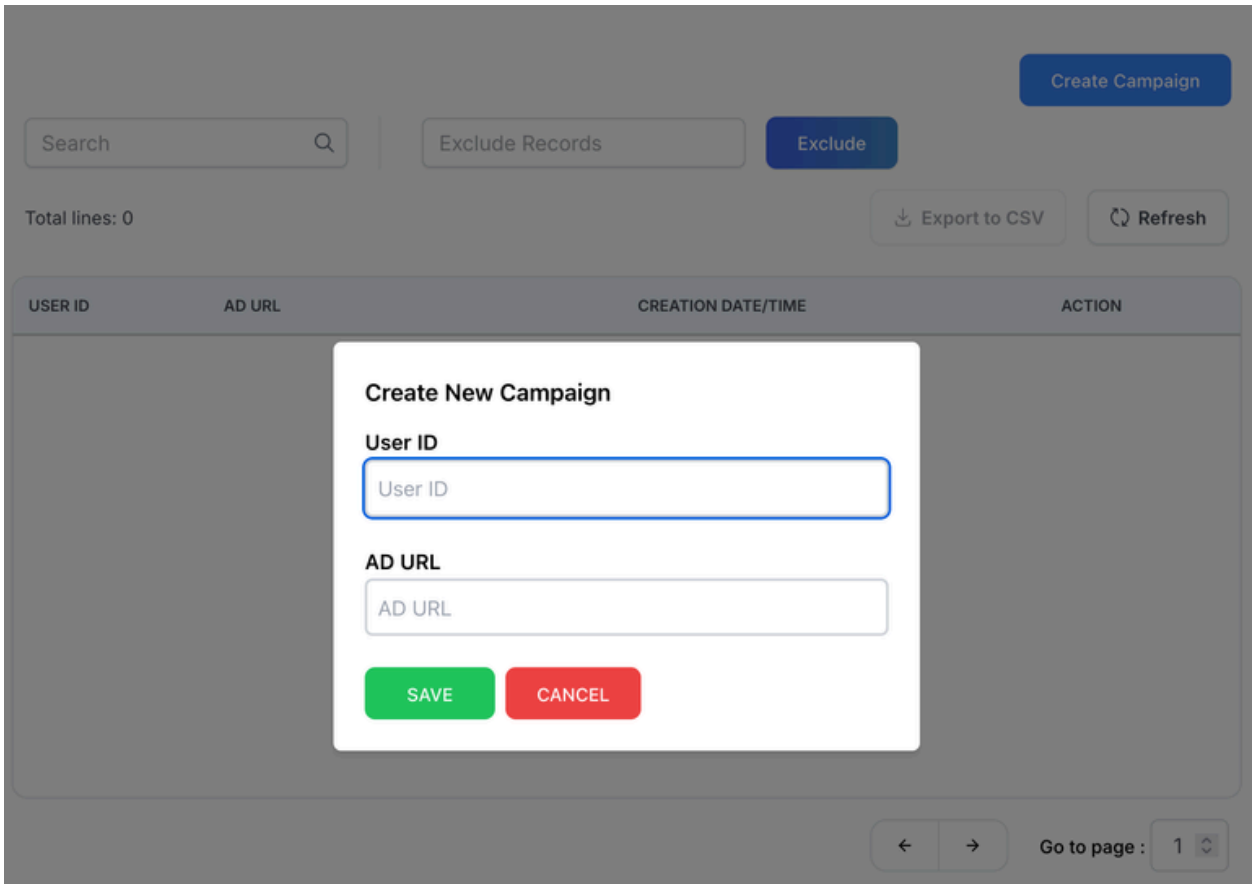


Figure 16: Screenshot of the “Mini Platform C” app.

We input a User ID, “test123” into this form, and an AD URL, “https://example.com/”, then we observed the tasking by visiting this NOAS URL:

```
https://events.platc-tester[.]com/cplatform/getAd?idfa=test123
```

The first time we visited it, the URL returned this:

```
var ifrm = document.createElement("iframe"); ifrm.setAttribute("src",
"https://example.com/"); ifrm.style="width:1px; height:1px; border:none;";
document.body.appendChild(ifrm);
```

Subsequent visits returned nothing.

This version of “Mini Platform C” does not appear to support any other options besides “Ad URL” for tasking the NOAS server. A similar version of the “Mini Platform C” app is also available on the site

`events-ui.discover-tech[.]io`. The JavaScript code for both app versions is available on archive.org (1, 2).

Additional Customer Mode Functionality

The Controlium platform provides several additional modules, according to our analysis of the app's user interface and source code.

Two Controlium modules named "Targeting" (also known as "Targeting Config") and "cTargeting" (also known as "Upload Audiences") allow users to upload digital identifiers referring to single or multiple targets, including mobile advertising IDs for Android and Apple devices, Beeswax user IDs, MyDSP user IDs and IP addresses. The "Targeting Config" module attaches the uploaded identifiers to a "segment", a widely used term that describes lists of identifiers to be used for targeting in digital advertising.

Controlium users can view data on ad impressions for a target identifier or IP address in the last 30 minutes:

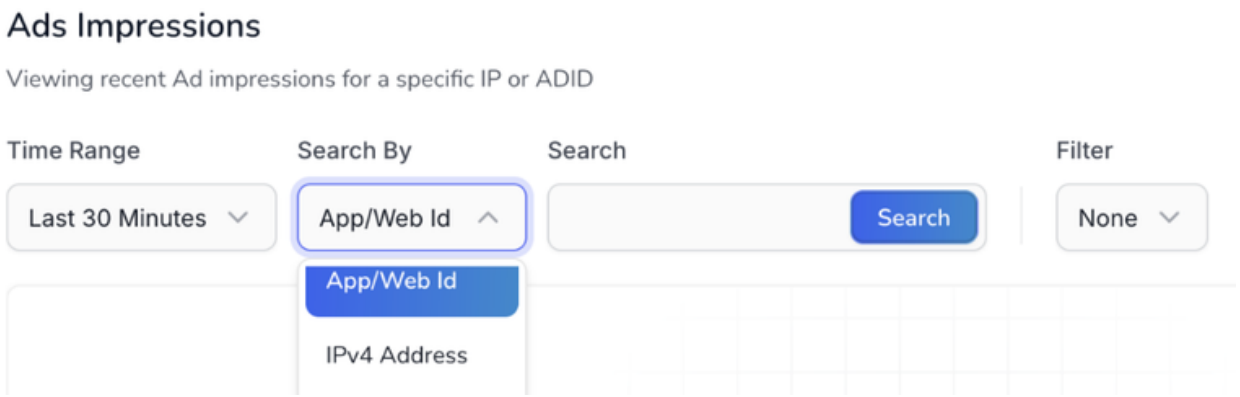


Figure 17: Screenshot of Controlium's "Ads Impressions" module.

A similar module named "Bid Requests" allows users to view data on recent ad bid requests for a specific target identifier or IP address. It provides a list of records that contain user IDs, the website visited or app used by the user, the IP address of the user's device and other attributes.

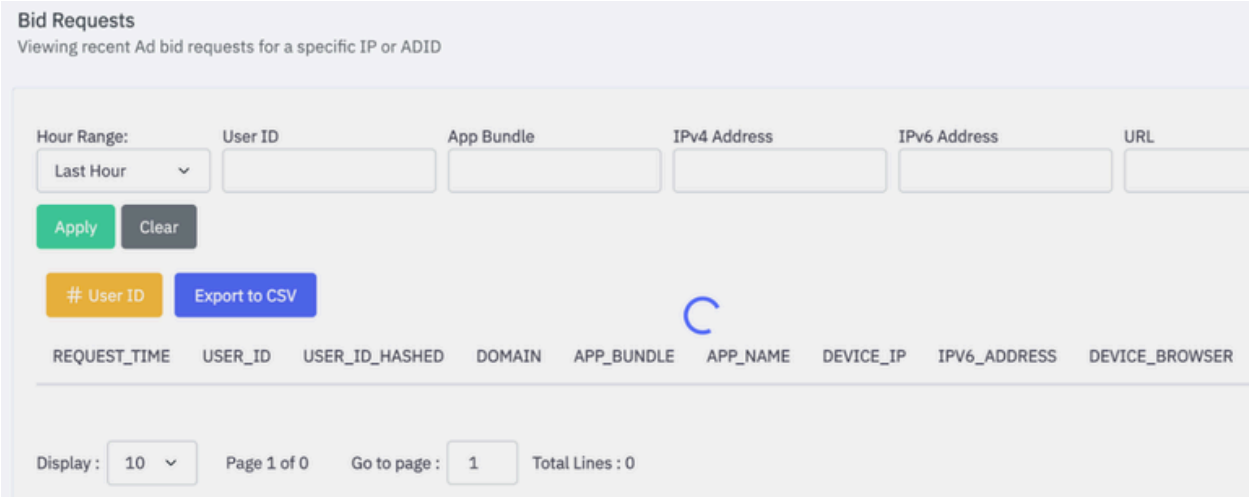


Figure 18: Screenshot of Controlium's "Bid Requests" module.

The "Events Logger" module provides access to activity records related to ad serving. The available data sources in another Controlium module named "OP Reporting" include MyDSP, Beeswax, Google, and Facebook. We are unsure what kind of reporting data would be displayed by that module. The "Ads Dashboard" module provides reports about ad impressions, the number of users reached and the amount spent (in $) for active campaigns.

Three Controlium modules named "User Info", "User API Info", and "User Sync Info" appear to provide key/value information on specific users upon entering user identifiers. They mention a number of attributes which we do not fully understand. For example, they offer to display user identifiers labeled "UUED" and "UUPD". One module provides a "User ID Type" selection. The available options include "EYield", "TYield", "VYield", "SYield", "Sync_User", "Sync_Domain", "Sync_App", "AH_User". Some of these options appear to be related to user ID syncing across different vendors, which is further examined in Section 6.

The modules that provide access to information on bid requests, ad impressions, events, and users can be used for troubleshooting and verification purposes, but also to spy on targets and other users whose data is in the bid requests.

4. Discover-Tech's Links with Mercenary Spyware, ADINT, and Mass Surveillance Vendors

This section examines links between Discover-Tech and the mercenary spyware companies Candiru and Bindecy. We also illustrate that, beyond facilitating mercenary spyware delivery, Discover-Tech is linked to ADINT firms, including Intelos. Discover-Tech also supports mass-deanonymization of internet and app

*users by a threat actor we call **DARK CARTOGRAPHER**, which exploits vulnerabilities in mobile networks to unmask users' phone numbers.*

Links with Candiru/Integrity Labs

We observed that Discover-Tech sends encrypted ad impression data to Candiru using Controlium's "Ad URL OpSec" feature. We identified several 2024 and 2025 Candiru infection links to at least six domains matching **Fingerprint V1** and that also contained a parameter "?q=" whose value was 16 bytes of data in Base64-encoded form. In every case, the value of the "?q=" parameter was correctly decrypted with the "V1" AES-256 key published on a page called "Ad URL OpSec Decoder" on the website `myipinfo[.]io`. The website `myipinfo[.]io` is clearly linked to Discover-Tech: passive DNS data shows multiple overlaps in IP addresses and CNAME records with other Discover-Tech websites, including `powerium[.]net` and `myweb3id[.]io` (see also Section 7).

One case of a Candiru infection link bearing a Discover-Tech *Ad URL OpSec* parameter is listed publicly on VirusTotal. The "?q=" parameter decrypts to an IP registered at the Saudi Ministry of Foreign Affairs, indicating that organization as a potential target of Candiru spyware via Discover-Tech ads:

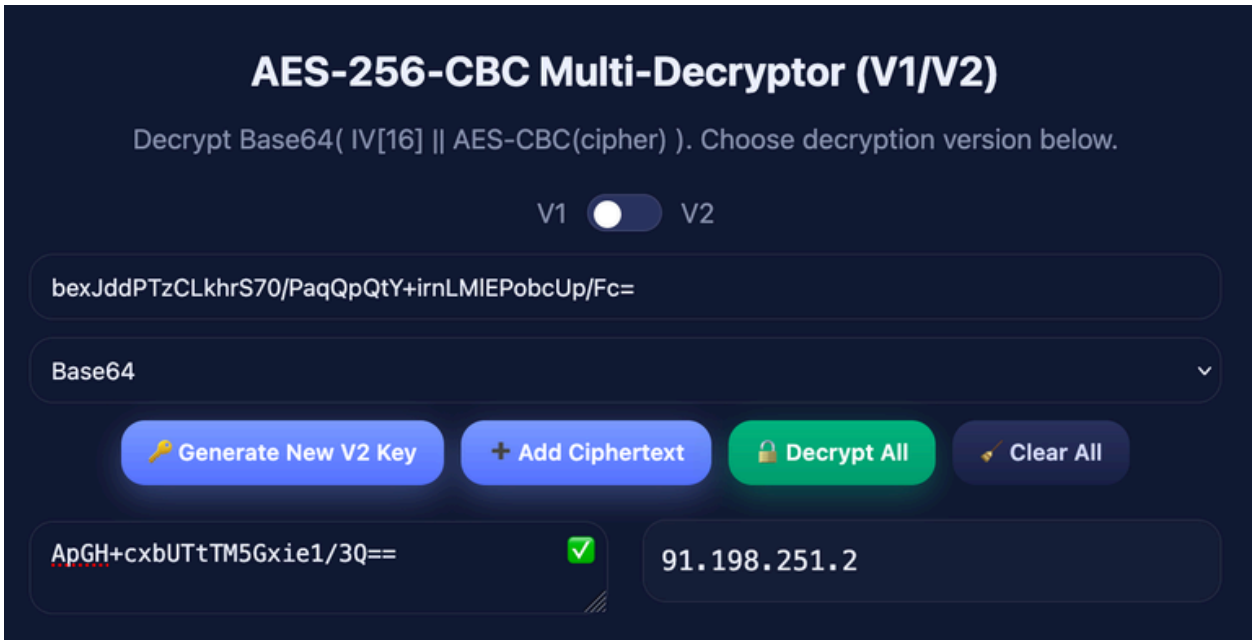


Figure 19: Discover-Tech's "Ad URL OpSec Decoder" shows that a Candiru infection link submitted to VirusTotal bears opsec data indicating the Saudi Ministry of Foreign Affairs as a likely spyware target.

We assess that this opsec data is included to facilitate a secure handoff from Discover-Tech to an attacker. The attacker presumably compares the visitor IP for the infection link against the IP encrypted

by Discover-Tech, to make sure the link from the ad impression was not silently swapped to a different device (as a security researcher might want to do to capture an exploit).

Tracking the Candiru/Integrity Labs Pre-Sales Team

Based on our analysis of Controlium user logins from an unauthenticated API endpoint (Section 3), we identified two users who logged in to Controlium from an IP address in Israel that we attribute to Candiru/Integrity Labs. One of these users, which we refer to as **INTEGRITYPRESALE1**, matched the name of someone listed on LinkedIn as having a "Head of Presale" position in Israel at "Cyber Security Company". The "Cyber Security Company" page is nominally for a Jakarta-based company, but we think the user selected this page because it has a generic name that conveys the industry in which they work without naming the specific company. Viewing the "Cyber Security Company" page on LinkedIn shows "Integrity Labs", "NSO Group", and "Integrity Lab" (apparently a typo of "Integrity Labs") in the top three spots in the "pages people also viewed" panel.

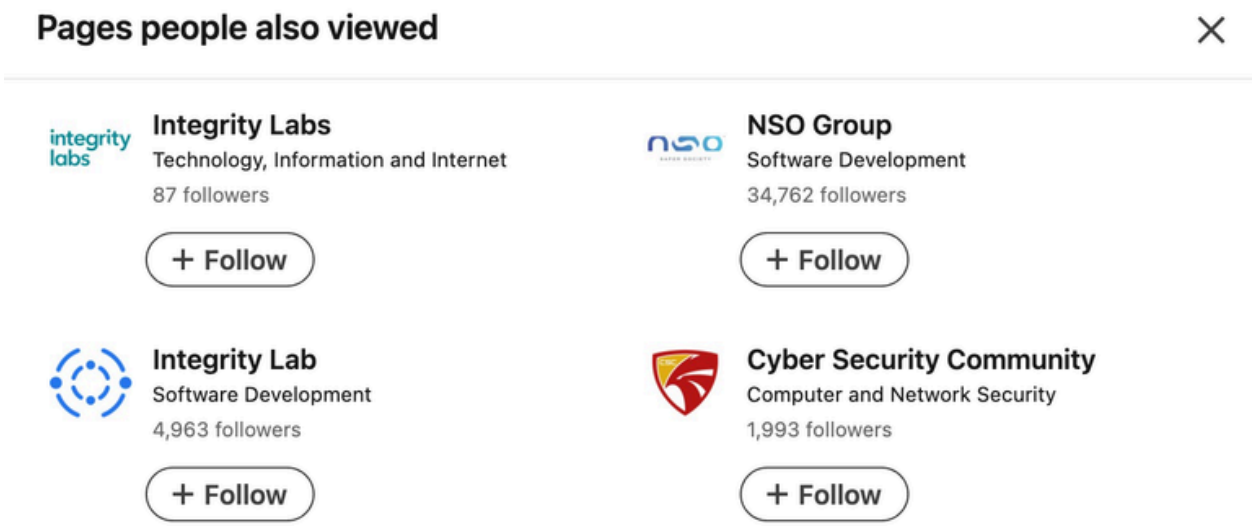


Figure 20: The page of Integrity Labs, as well as a typo version both appear in "Pages people also viewed" for "Cyber Security Company" on LinkedIn.

The second user signing in from the Integrity Labs IP address, which we refer to as **INTEGRITYPRESALE2**, has a username that appears to include a first name, and ends in "_pap_pres". We suspect the "_pres" stands for "presale". There is a user on LinkedIn who shares a first name with this user, and is a "Presales Engineer" at "Cyber Security Company", though we cannot be certain it is the same individual.

We identified **INTEGRITYPRESALE1** and **2** signing into Controlium from locations in the following countries: Azerbaijan, Czechia, Israel, Italy, Mexico, Montenegro, UAE, and the United States.

We are unsure what the phrase “pap” refers to, but we noted only two other usernames that contained the string “pap”. They were part of a cluster of users signing in exclusively from the local IP address 10.0.0.52, suggesting these as further possible Candiru-linked users:

```
Aurora_api, Barbara, Chameleon, CS, Fox, Heron, Journey, MobyDick, Oris,
papdev2, papplayg, Presale, Scorpion, spare2
```

Candiru’s Profiling Servers

While tracking Candiru’s infrastructure in 2025, we noticed that two domain names that matched our **Fingerprint C1** were registered within two hours of each other on March 18, 2025 with `info@rockhoster[.]com` in their SOA record:

```
outdooutcome[.]com
suggestutterly[.]com
```

A third domain that looked similar was registered on March 18, 2025 within the same timeframe, also with `info@rockhoster[.]com` in its SOA record, but it *never matched* our Candiru fingerprint:

```
sincereaccertain[.]com
```

However, we noted that starting in April 2025, URLs pointing at `sincereaccertain[.]com` were distributed via Discover-Tech ads. The URLs looked like this:

```
https://sincereaccertain[.]com/?qq=[...]
```

The qq parameter contained Base64 data. Pasting the Base64 data into Discover-Tech’s “Ad URL OpSec Decoder” (see above) resulted in a successful decrypt using their “V2” AES decryption scheme. The decrypted data looked like this:

```
<IP>|<Timestamp>|<User-Agent>|<Ad-ID>
```

In May 2025, we observed `d1fcoizt7mje85.cloudfront[.]net` with URLs and data that decrypted to the same format. We conclude that `sincereaccertain[.]com` is linked to `d1fcoizt7mje85.cloudfront[.]net` because URLs to both domain names appeared to be distributed via the same *Infinite FIFO* ID, number 778. Deployment of the `d1fcoizt7mje85.cloudfront[.]net` URLs appeared to cease in December 2025. We estimate that between hundreds of thousands and millions of users were directed to these domains via Discover-Tech ads.

We identified no similar activity until January 2026, when Discover-Tech appeared to evolve their *Infinite FIFO* feature. The NOAS URL associated with these new Infinite FIFOs was `ppv2[.]mtrtb[.]com`. We were able to gather statistics from an unauthenticated endpoint on this server for five months between January 2026 and June 2026, when Discover-Tech removed the unauthenticated endpoint. The statistics counted (among other things) the number of "eligible users", which appeared to be the number of users who were directed to `ppv2[.]mtrtb[.]com` *and* who were intended to receive some infinite FIFO code. We counted a total of 3,637,213 eligible users during this period, though we note that it is possible that Discover-Tech customers other than Candiru may make use of the Infinite FIFO feature.

Later in 2026, we noted a migration to what we assess is "V3 OpSec", which allows a custom name to be specified for the parameter instead of "qq" (we noted "impid"), and a per-user key. Discover-Tech neglected to update their "Ad URL OpSec Decoder", so we were unable to decrypt this data.

We were unable to obtain any of the JavaScript code from sincereaccertain[.]com or these CloudFront distributions, likely because of *Discover-Tech's Ad URL OpSec* feature, though we note that Confiant was able to obtain related code.

Bindecy

Based on our analysis of user logins from an unauthenticated API endpoint (see Section 3), we noted that two users, **maya** and **mayaqa**, were logging into Controlium from multiple IP addresses including an IP address in Israel `62.90.129.xxx`. We noted that this IP address was administering multiple websites that had self-signed certificates issued by "**cupid-ca**":

```
beachvibesnow[.]com
enjoymultiplecats[.]com
icecreamtester[.]com
```

We identified a total of seven certificates on Censys issued by "`cupid-ca`". Other domain names included `pickarest[.]com` and `infoanalytics[.]live`. Both pointed to IPs that returned a distinctive speedtest page on port 8443 without TLS:

```
services.http.response.body_hashes="sha256:63c2963a7abc1e4ee083275e5582a52f110
1dba9905fd35498726359abf95a71"
```

One of the IPs that matched this same fingerprint was 52.174.65.77, while it was pointed to by the domain:

```
archer.westeurope.cloudapp.azure[.]com
```

Other domains pointing to the same IP were connected to a Heroku app:

```
bd-mainserver.herokuapp[.]com
```

From talking to our partners, we understand that Bindecy has products called “Archer” and “Cupid”. We believe the “bd” in “bd-mainserver” may also be a reference to Bindecy.

Some of the domain names we mapped to Bindecy were registered in the name of an Israeli software company, Moveo Group. Additionally, one of the domain names appeared to be a domain name bearing the name of an Israeli web developer and entrepreneur without any obvious connection to Bindecy.

We were able to fingerprint Bindecy’s servers and identify locations of some Bindecy operators: Belgium, Germany, Norway, Portugal, Sweden, Singapore, and Spain. We also identified a customer that appeared to be using Bindecy’s spyware in Mexico and Colombia, but were not able to determine the location of the operator.

We further discuss the Israeli spyware vendor Bindecy and its corporate network in Section 8.

Bindecy did not respond to our request for comment within the timeline provided.

Links with Intelos, DARK CARTOGRAPHER, and Other Vendors

Intelos

Based on our analysis of user logins from an unauthenticated API endpoint (Section 3), we identified several users logging in to Controlium from IP addresses that returned certificates for `globaldatapoints[.]com`. We identified passive DNS data showing a CNAME record for a subdomain of `globaldatapoints[.]com` that contained the word “Intelos”.

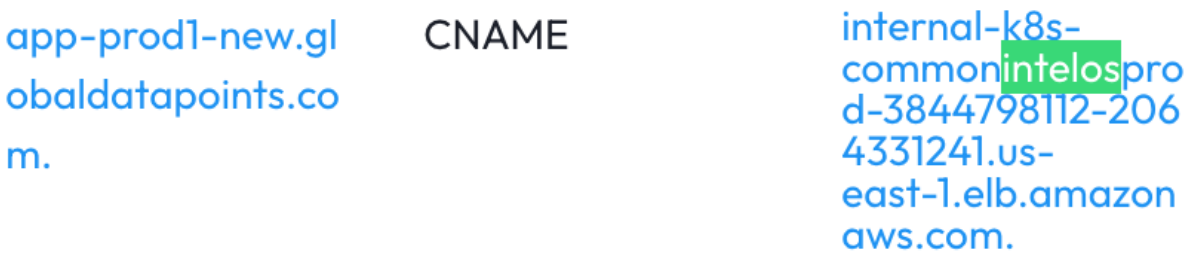


Figure 21: A subdomain of `globaldatapoints[.]com` contains a CNAME record to an AWS Elastic Load Balancer whose name contains the string "intelos".

Furthermore, a subdomain of `globaldatapoints[.]com` briefly returned a login page for an application called "AD/HOC," which has been reported to be the name of an Intelos product.

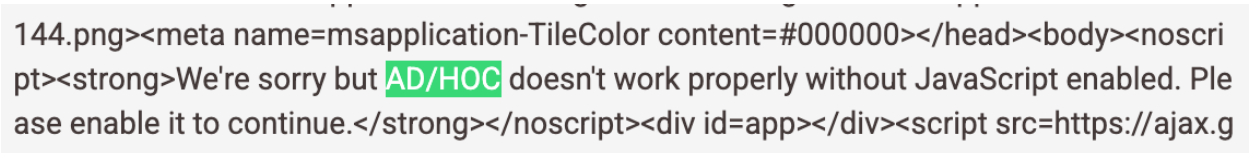


Figure 22: An IP pointed to by a subdomain of `globaldatapoints[.]com` returned an app called "AD/HOC".

We identified at least 15 Controlium users that we believe are linked to Intelos. **Table 1** shows users that signed in from locations that did not appear to be VPNs or proxies:

Username	Sign-ins from
bear	Belgium, Israel, Singapore, Poland
timtamteam64	Israel, Spain
liinine77263, johny7716243	Macedonia
Landrover	Spain
bear_solo	Hungary
carpe_eb	Israel, Portugal, UAE
rollsgreen1	Spain
JonG	Belgium, Czechia, Greece, France, Israel, Italy,

	Serbia
mishreg	Israel, Latvia
Barhi	Israel, Thailand
metalica1	Belgium

Table 1: Controlium sign-ins from Intelos-linked users.

The mercenary ADINT vendor Intelos, which reportedly offers both ad-based geolocation surveillance and the delivery of spyware via ads, has additional links to Discover-Tech via Intelos shareholder Eric Banoun (2018 – present), who was also a director of Discover-Tech (2020 – 2025), as detailed in Section 8.

Intelos did not respond to our request for comment within the timeline provided.

DARK CARTOGRAPHER: Mass-Deanonymization With Ads

We identified Discover-Tech ads that sought to exploit the well-known "WebRTC IP Leak" issue, which can potentially reveal the IP address of VPN and proxy users. The same ads also attempted to unmask the phone number (MSISDN) of mobile users who were served the impression. The MSISDN leaks exploit various issues, including widespread problems with so-called "zero-click login" technologies, which aim to facilitate frictionless authentication and purchases for users on their mobile devices.

One way "zero-click login" operates is that mobile providers select certain websites for "HTTP header enrichment," so that when plaintext HTTP requests pass through the provider's mobile gateway, an HTTP header (like X-MSISDN) is added to the request that provides the user's phone number to the website. As an alternative to HTTP header enrichment, third-party services may work directly with the telco to facilitate this "zero-click login". There appear to be widespread bugs with this allowlist matching, as well as bugs or security issues in third-party enrichment providers. While mainstream web browsers such as Chrome are moving towards blocking any non-HTTPS requests, it is likely that the app ecosystem will still embed webviews that permit non-HTTPS content.

We taxonomized the issues into five types, exploited by attackers across numerous mobile providers in more than 30 countries in North America, South America, Europe, Africa, and Asia, and disclosure to companies is in progress. Once the disclosure process is complete, we will release our subsequent report delving into technical analysis and attribution of these attacks.

Notably, **DARK CARTOGRAPHER**'s infrastructure links to both a mercenary adtech vendor and a U.S. government contractor. It is rare to see such direct overlaps between mercenary vendors and U.S. government or intelligence contractors. We assess that this attacker has been exploiting MSISDN leak

issues since at least 2019, fronted by a variety of mercenary adtech companies. Our investigation into this threat actor is ongoing.

Other Vendors

We found a number of Controlium users that we could not conclusively attribute to a specific company: the user **mi19mos25a** primarily logged in from India, and occasionally Israel; the user **rcs1** exclusively logged in from Italy, primarily a static IP in Milan; the user **Pindi** exclusively logged in from Pakistan.

5. Uncovering Discover-Tech's Billion-Bid Scale Ad Targeting

To understand the scope of Discover-Tech's activity, we analyzed nearly four billion ad bidding records that were publicly exposed on a Discover-Tech website. We found that Discover-Tech ads were displayed in over 70,000 mobile apps, and over 120,000 websites between March and June 2026.

We found two world-readable Apache Druid instances running on Discover-Tech's website `mtrtb[.]com`. The `druid.mtrtb[.]com` endpoint contains bidding data for Discover-Tech's MyDSP platform, which is connected to several upstream ad providers including Google, Yandex, Vungle, and Sunteng. The `cn.druid.mtrtb[.]com` endpoint appeared to contain additional bidding data for Discover-Tech's use of Sunteng. These instances did not contain any information about Discover-Tech's use of Beeswax or Eskimi DSPs. Discover-Tech appeared to shut down both instances in August 2026.

There were no instances of cookie IDs, advertising IDs, or GPS coordinates recorded in the Druid data. However, the data includes IP addresses or /24s, presumably provided by SSPs, as well as city-level geolocation information. The provenance of the location data is unclear.

What Upstream Ad Providers Does MyDSP Use?

MyDSP appears to make use of several upstream ad providers, which are listed in the "exchange" field of the database. We identified five distinct values.

Exchange	Share of Bids
YANDEX	67.4%
GOOGLE_AD_MANAGER	24.74%
VUNGLE	7.24%
GOOGLE_RETARGETING	0.05%
SUNTENG	0.03%

Table 2: Share of MyDSP bids by the value of the "exchange" column.

No Good Evidence of Legitimate Ads

We reviewed bidding data for MyDSP for four months (March through June 2026). In this period, Discover-Tech's MyDSP bid on 3,770,286,576 impressions, and appeared to win 441,954,291 (11.7%). About 76.7% of the bids were for ad impressions in mobile apps, and 23.3% for impressions in the web browser.

The database shows a total of three advertisers, with nine total combinations between advertiser and an advertiser domain name. Most of the advertisers seem to be directly attributable to Discover-Tech itself, or to entities we consider to be linked to it, like Akedo, MyIPInfo, and Volasim's RemindMeWhere app.

Advertiser	Advertiser URL	Share of Bids
discover-tech	akedo.gg	37.31%
AliExpress	www.aliexpress.com	34.70%
MyIPInfo	https://myipinfo.io	12.65%
discover-tech	www.remindemewhere.app	9.61%
discover-tech	www.aliexpress.com	3.57%
discover-tech	https://myipinfo.io	1.36%
discover-tech	s.taobao.com	0.79%
discover-tech	https://aliexpress.com	0.01%
discover-tech	https://king.com	0.01%

Table 3: Share of MyDSP bids by the value of the "advertiser" column.

The database records that MyDSP spent approximately **$109,091** in this period, assuming the cost is recorded in micros of USD. The database appears to be set up to record information about the revenues and profits generated by MyDSP for each ad, including fields like **advertiser_revenue**, **dsp_profit**, and **margin**, but these are always set to zero except for a three-day period in June where **advertiser_revenue** is nonzero for impressions shown for the MyIpInfo advertiser. The database also contains fields to record conversions, though these are always set to zero. A "conversion" typically refers to a purchase, app install or other action taken by a person who was exposed to an ad. It is highly

unusual for an ad vendor that not a single ad leads to such an action, although it is conceivable that the bidding records might not track and record this information.

We reviewed ads for the major advertiser on this list that could hypothetically be a real external advertiser, “AliExpress.” The ads all appear to be a generic image that says “SALE” and shows a picture of miscellaneous products from Ugreen, a Chinese consumer electronics company.



Figure 23: A large version of the AliExpress/UGREEN “Sale” creative used across multiple Discover-Tech campaigns.

We note that the landing page of some of the AliExpress ads is an AliExpress affiliate link.

```
https://s.click.aliexpress[.]com/e/_c3U5aNwL
```

We have no evidence of a business relationship between Discover-Tech and AliExpress and/or Ugreen, and we think the generic nature of the advertising content, the lack of any revenue recorded, and the lack of any conversion data recorded suggest these ads were likely not purchased on behalf of AliExpress or Ugreen.

Normally, a DSP would aim to earn money by selling ads to entities seeking to advertise goods and services. In this case, there is no good evidence that Discover-Tech’s MyDSP is earning money in this way.

Evidence of Ads With Attacker Script Tags

The MyDSP data shows that at least 718,748,885 of the bids (about **19%**), were to show ads that apparently contained a script tag pointing to a NOAS server. We believe that the NOAS server is, generally, tasked to return some JavaScript exactly once to specific mobile ad ID and/or browser/cookie ID values, and subsequent visits return nothing until re-tasking.

We assessed whether an ad was likely to contain such a script tag by searching for ads whose name included the strings “infi” (a reference to Controlium’s “Infinite FIFO” feature), “NOAS”, “ppv2”, and “pqv2”. The “ppv2” and “pqv2” strings appear to be references to a newer version of the “Infinite FIFO” feature exposed as “Authenticator Manager” in the Controlium UI. We suspect that “pqv2” is for testing and/or QA, whereas “ppv2” is for production.

MyDSP submitted bids to show these NOAS ads to users with IP addresses that geolocate to 161 countries. It is important to note that IP geolocation can be inaccurate due to the use of satellite providers, VPNs, or other reasons.

Country	Bids
Yemen	457,283,658
Pakistan	139,427,322
Montenegro	97,595,716
Brazil	76,108,495
Mexico	32,675,229
China	30,072,952
Belarus	25,122,945
Armenia	23,189,997
Czechia	19,107,486
Israel	18,477,493

Table 4: The top 10 countries by raw bids.

Country	Bids Per Capita

Montenegro	156.68
Yemen	13.99
Armenia	7.49
Latvia	3.14
Seychelles	3.13
Belarus	2.77
Israel	1.80
Czechia	1.75
Denmark	0.99
Azerbaijan	0.97

Table 5: The top 10 countries by bids per capita.

Looking at the full bidding data, without considering whether ad auctions were won, MyDSP also made a significant number of bids (> 10 million) on ad impressions geolocated to Russia, Indonesia, United Arab Emirates, Australia, United States, Sweden, Norway, Netherlands, Germany, Malaysia, and Cuba. However, we note that the Netherlands, Germany, and United States geolocation appeared to primarily be from VPNs or server IPs in these countries.

Apps and Websites That Displayed the Ads

Ads with attacker script tags were shown to users of 75,373 different Android and iOS apps and to visitors of 120,768 different websites in mobile and desktop browsers. These numbers refer to ads actually displayed to users of apps and websites rather than raw bids.

Android apps that displayed more than one million of those ads include MX Player and Lark Player:Music Player & MP3. The messenger Viber showed more than 700,000. The apps Snap VPN, Truecaller, and VivaCut – AI Video Editor displayed around half a million. The ads were deployed in email apps like Yahoo Mail, browser apps like Opera Mini, weather apps like German Wetter Online, learning apps like Duolingo, religious apps like WeMuslim, health apps like Period Calendar Period Tracker and in a large number of games like Bubble Shooter and Ludo STAR. Lower numbers of ads in the thousands were shown in family tracking apps like Location Share and in dating apps like Badoo and Grindr.

iOS apps deployed fewer of those ads than Android apps. The messenger Viber, which ranks second on iOS, showed only around 200,000 ads as compared to around 700,000 on Android. Still, the ads were displayed across a similarly wide range of iOS apps.

As discussed above, Discover-Tech's ad targeting appears to focus on mobile apps. Only 23.3% of the bids we analyzed were for ad impressions in the web browser. Websites that displayed more than one million ads with attacker ad scripts include news publications from Armenia (`mamul.am`) and Serbia (`kurir.rs`). More than 100,000 of those ads were shown on news publications and other popular sites from Montenegro (`dan.co.me`, `vijesti.me`), Yemen (`adngad.net`), and Pakistan (`whatmobile.com.pk`). The site Weather.com displayed around 400,000. Larger numbers of ads were also shown on `yahoo.com`, `AccuWeather.com`, `tripadvisor.com`, `yandex.ru`, and news sites in Denmark (`bt.dk`), Bosnia (`slobodna-bosna.ba`), Egypt (`almasryalyoum.com`), and Kazakhstan (`vesti.kz`). The long tail of websites that deployed those ads included everything from `9gag.com` and `foxnews.com` to `bbc.com`, `cbc.ca`, `haaretz.co.il`, and `nytimes.com`.

Ad Impression Data Highlights Systemic Risk

Our review of the ad bidding data indicates that Discover-Tech ads were shown on devices in national-security-sensitive networks around the world. These include the networks of various ministries of defense, armed forces, national cyber agencies, intergovernmental organizations and multilateral security organizations including NATO, and networks associated with critical infrastructure. The data also show impressions from the networks of media organizations around the world. At minimum, we assess that these ad impressions would have resulted in profiling by Discover-Tech. In some cases, the impressions could have resulted in code from Candiru or other entities running on the user's device.

A Discover-Tech ad impression does not in and of itself confirm targeting or infection with spyware. However, the fact that Discover-Tech was able to bid on and show ads on these networks highlights the systemic risk posed by AdFection and the advertising ecosystem, and warrants urgent investigation to determine whether any users on these networks were infected with spyware. We also note that our visibility into Discover-Tech's impressions is confined to the data on Discover-Tech's MyDSP platform. This data does not include data from Beeswax and Eskimi, and covers a limited time period. This incompleteness further reinforces the need for follow-up investigation.

NATO and the United Nations

We identified impressions in NATO and United Nations networks.

European Union Entities

In Europe, we identified impressions from the networks of the European Parliament, the European Commission, and the Council of the European Union's General Secretariat.

Nordic Government & Critical Infrastructure Clusters

We identified widespread impressions in Nordic states, including Denmark, Norway and Sweden. We assess that this cluster warrants close scrutiny, and note some of the more concerning findings:

- **In Norway**, Discover-Tech ads were shown to users on the networks of the legislature (Stortinget), the Norwegian Digital Agency (Digitaliseringsdirektoratet), the Norwegian Communications Authority (Nasjonal kommunikasjonsmyndighet), state IT networks (Statens IT), the Norwegian Police (Politiets It-enhet) and serious crime units (Kripos), among many others. Notably, we also identified impressions in multiple county and municipal networks across northern Norway, including near key military installations (e.g. Alta, Harstad, Nordland).

- **In Sweden**, Discover-Tech ads were shown to users on the networks of the Armed Forces, the national grid operator (Svenska Kraftnat), the state owned power company (Vattenfall AB), the national internet exchange (Netnod AB), defense contractor Saab, Volvo Group, university networks including the Chalmers University of Technology, national research funding bodies (Verket for Innovationssystem), and Sweden's national Meteorological and Hydrological Institute (Sveriges Meteorologiska och Hydrologiska Institut).

- **In Denmark**, Discover-Tech ads were shown to users at the national rail network (Banedanmark), the national post (Post Danmark), Denmark's National Research and Education Network (Forskningsnettet), alongside multiple municipal and regional government networks and public health authorities. They were also shown on networks at Denmark's digital infrastructure company KMD A/S, renewable energy sector firms such as Vestas Wind Systems and Ørsted, Grundfos, banks including Den Danske Bank, and Copenhagen Airports.

Australia: Critical Infrastructure, Government & University Networks

The ad impression data also reveal a substantial cluster of impressions in Australia, including on government and private-sector networks associated with critical infrastructure sectors like grid and power companies, as well as networks associated with universities and research centres, including entities working on nuclear research, like the Australian Synchrotron, and the Australian Nuclear Science and Technology Organisation.

Governmental Targets: A Global List

Numerous other geographically distinct clusters of widespread impressions appear among the data. Many of these impressions occurred in defense, foreign affairs, internal affairs, or security bodies. **Table 6** provides examples of the government networks where we found Discover-Tech impressions.

Government	Examples of networks with Discover-Tech impressions

Armenia	Central Electoral Commission Central Bank Office of the Price Minister
Czechia	Ministry of Finance Ministry of Foreign Affairs Ministry of the Interior State Institute for Drug Control Czech Telecommunication Office Ministry of Agriculture The Czech National Bank Ministry of Labour and Social Affairs Municipal Office, Prague National Cyber and Information Security Agency
Israel	Ministry of Health Ministry of Foreign Affairs Government ICT Authority Ministry Of Defence Israeli Police Bank of Israel Israel Internet Association Israel Airports Authority
Italy	Bank of Italy Parliament (Camera dei deputati) Ministry of Defense

Table 6: Examples of government controlled or operated networks where we identified Discover-Tech impressions.

Our investigation is ongoing. As of now, we have identified impressions in government-operated networks in the following countries:

- Armenia (including the Office of the Prime Minister)
- Australia
- Azerbaijan
- Bhutan
- Brazil
- Czechia
- Denmark
- Indonesia
- Israel
- Italy

- Kosovo
- Libya
- Malaysia
- Mexico
- Montenegro
- Norway
- Pakistan
- Russia
- Somalia
- Sweden
- Thailand
- The United Arab Emirates
- The United States (American Samoa)
- Uruguay

We also found impressions on the networks of election oversight bodies in Armenia, Indonesia, and Mexico.

Chips & Semiconductors: From Research to Fabrication

We found what appears to be a nexus among the advanced semiconductor industry, covering the chain from design, memory, to chip development and fabrication, with the greatest number of impressions seen in Intel networks, alongside Nvidia, Sandisk, Texas Instruments, Broadcom, Micron Technology, and ARM. We also identify numerous research entities in this category like IMEC. We also identified impressions within the networks of large U.S. tech firms including Apple, Microsoft, and Motorola.

We also identified impressions in specifically defense-sector tech entities, including Raytheon (U.S.) and Elbit Systems LTD (Israel), and the nuclear sector, including the Westinghouse Electric Company (U.S.).

Global Media Organizations

Given our identification of zero-click attacks against Al Jazeera, we scrutinized bidding records for impressions within the networks of media organizations. We found many. Often, these included the largest media organizations in a particular country, as well as public broadcasters and media conglomerates. The countries (with a count of institutions) include:

- Australia: 3
- Denmark: 3
- France: 1
- Mexico: 2
- Israel: 3
- Italy: 2
- Norway: 2

- Sweden: 3

We also identified impressions within the networks of international media services. Our investigations into these cases are ongoing.

Confiant's Findings Underscore Dangers of AdFection

The researchers at Confiant analyzed targeting data and found signs that these ads were displayed on networks of major governmental entities, including the U.S. Department of Defense, the Dutch Ministry of Economic Affairs, Estonia's Information System Authority (RIA), Spain's Ministry for Digital Transformation and Civil Service, Armenia's Office of the Prime Minister, and multiple government entities in Israel. Their research also found signs they were shown in networks of the International Atomic Energy Agency (IAEA) and the International Criminal Court.

6. How Discover-Tech Deploys Ads in the Browser

In this section we show how, beyond targeting users of mobile apps, Discover-Tech deploys a range of techniques to deliver ads and track users while they browse across websites. This involves Discover-Tech running its own code in the user's web browser, both while deploying ads to users and independently of showing them ads. We explore Discover-Tech's "Banner Tester" tool to show how the company generates tracking tags and pixels attached to ads, including code that connects to a NOAS server, which we identified as a vector for spyware delivery. We also document how Discover-Tech engages in "ID syncing" with other ad vendors, and how it leverages IAB Europe's "Transparency and Consent Framework" to appear GDPR-compliant, even while facilitating unwanted and malicious activity.

An ad displayed to a website visitor consists of an image or video to be shown and a link to be clicked, but can also carry HTML and JavaScript code that connects to one or more domains in order to track users, ad impressions, clicks, and other activities. This code is typically referred to as an ad tag. A related concept, a so-called tracking pixel, also describes code running in the web browser that connects to third-party ad vendors. Ad vendors use additional tracking code for user ID syncing by exchanging user identifiers with each other in order to identify, profile, and target website visitors across sites and vendors.

Our analysis of ad tags, tracking pixels, and ID syncing activities associated with Discover-Tech's ad delivery is based on an analysis of publicly available code, browser testing and ad transactions archived by the web investigation tool urlscan. While ads displayed in mobile apps similarly carry code that connects to ad vendors, this section focuses on Discover-Tech ads displayed in the web browser.

Discover-Tech's Ad and Tracking Tags

We found two versions of another app related to Discover-Tech's Controlium platform named "Banner Tester" published on the sites `bt.myweb3id[.]io` and `bt.platc-tester[.]com`. The apps provide the ability to generate and preview tags for banner ad campaigns in the browser.

The generated tags contain an ad creative and a link, which appear to serve testing purposes:

```
<a href='https://s.click.aliexpress.com/e/_DFudZEL' target='_blank'
onClick='clicker();'><img
src='https://cloud-images.s3.eu-west-1.amazonaws.com/MyDSP_Beeswax/Ali_rt_shop
/320x50_1.png' id='222233'></a>
```

The tags contain additional HTML and JavaScript code that is prepared to make a number of requests to different URLs, including NOAS URLs and URLs for ad impression and click tracking. One version of the app generates tags for the "Target" platforms "Default" or "Mini Platform C". The other version can generate tags for production, staging and testing environments, according to its source code. The generated ad tag URLs differ depending on the chosen options.

	Ad tag URLs for different platforms and environments
NOAS URL	noas.mtrtb.com/getAd events.myweb3id.io/cplatform/getAd noas.powerium.net/getAd qa-noas.powerium.net/getAd
Event tracking URL	logger.controlium.net/register_event
Impression tracking URL	dtech.adtimizer.co/DSPCLogger/Impoint imp.powerium.net/DSPCLogger/Impoint tracker.mtrtb.com/tracker/imp/
Click tracking URL	dtech.adtimizer.co/DSPCLogger/ClickProcessor imp.powerium.net/DSPCLogger/ClickProcessor tracker.mtrtb.com/tracker/click

Table 7: Ad tag URLs generated by Discover-Tech's "Banner Tester" app.

As the impression and click logging URLs generated by the app contain the parameter "dsp=BW", we assume that these ad tags are designed to be deployed via the DSP Beeswax.

Several records archived on urlscan show examples of how Discover-Tech actually deployed very similar ad and tracking tags during visits to websites:

- During a visit to the Russian literature website `livelib[.]ru` in May 2025, Discover-Tech delivered an Akedo ad via its ad system MyDSP and Yandex, including requests to `noas.mtrtb[.]com` and `dtech.adtimizer[.]co` (urlscan).
- During a visit to `nbcnews[.]com` in August 2025, Discover-Tech delivered an Akedo ad via its ad system MyDSP and Google, including requests to `tracker.mtrtb[.]com` and `dtech.adtimizer[.]com` (urlscan).
- During a visit to a Spanish-language horoscope site in July 2025, Discover-Tech delivered a MyIPInfo ad via Beeswax DSP and Google, including requests to `infinoas.mtrtb[.]com` and `dtech.adtimizer[.]co` (urlscan).

User ID Syncing with Other Ad Vendors

Unlike apps on mobile devices, web browsers do not allow websites to access a universal device identifier. The process of "ID syncing", often also referred to as "cookie syncing", addresses this lack of a universal user identifier. Research shows that digital advertising firms and data brokers use sophisticated forms of ID syncing to identify, profile and target web users across vendors. They achieve this by constantly exchanging user identifiers with each other, storing them in the browser and retrieving them again while users visit different websites that embed third-party tracking code.

We found evidence showing how Discover-Tech engages in ID syncing with Comcast's ad system Beeswax, Yandex, and Microsoft's ad platform Xandr.

Discover-Tech appears to use its `myweb3id[.]io` domain for ID syncing with Yandex. This domain is highly prevalent as a tracking domain on a large number of websites. Starting in May 2025, urlscan archived more than 10,000 records that include third-party requests to the domain `events.myweb3id[.]io`, most of them occurring during visits to Russian websites.

A recent urlscan record shows an example of a typical request chain that involves ID syncing across Discover-Tech's `events.myweb3id[.]io` domain and the following Yandex endpoint:

```
an.yandex.ru/mapuid/discovertechis
```

The URL component "discovertechis" indicates some kind of business relationship between Discover-Tech and Yandex.

Discover-Tech appears to use another domain, `tracookiepixel[.]xyz`, which is associated with `myweb3id[.]io` via DNS links and which is also highly prevalent as a tracking domain on a large number

of websites, for ID syncing with Beeswax. Starting in July 2025, urlscan archived more than 10,000 records that include third-party requests to `tracookiepixel[.]xyz`, many of them occurring during visits to popular websites including IMDb and New York Times.

A recent urlscan record shows an example request chain that was initiated during a visit to the website of The Guardian, which involves ID syncing across Discover-Tech's `tracookiepixel[.]xyz` domain and Beeswax' tracking `domain bidr[.]io`. The requests contain the parameter "bee_sync_partners=dtech", which indicates some kind of business relationship between Discover-Tech and Beeswax.

These ID syncing activities typically take place during website visits even when a user was not served a Discover-Tech ad. We are unsure how exactly Discover-Tech uses its browser ID syncing capabilities. Generally, being able to synchronize and correlate user identities across vendors is considered a precondition for individual-level ad targeting in the web browser. The Controlium platform, as examined in Section 3, offers to upload lists of Beeswax identifiers for ad targeting in its "cTargeting" module, among mobile advertising IDs, IP addresses, and other identifiers, based on our analysis of the source code.

We conclude that many websites make constant requests to Discover-Tech's domains `events.myweb3id[.]io` and `tracookiepixel[.]xyz` in the background. These requests serve the purpose of ID syncing with Beeswax and Yandex, and Discover-Tech's domains receive, in addition to user identifiers, at least the website visitor's IP address and information about their browser and operating system.

Discover-Tech's Tracking Pixel

Separately from Discover-Tech's large-scale ID syncing on many websites, we found JavaScript code for a "tracking pixel" that was loaded during recent visits to only a few sites including `myipinfo[.]io`, `cookiesurfer[.]com`, and Discover-Tech's corporate website, `discover-tech[.]io` (all three archived on urlscan).

These sites loaded versions of the tracking pixel code, both broadly similar, from the following URLs:

```
js.tracookiepixel.xyz/myipinfo/c_tracking_pixel_gdpr.js
js.tracookiepixel.xyz/dt/c_tracking_pixel_gdpr_enhanced.js
```

Based on our analysis of the source code, the tracking pixel serves the purpose of storing, retrieving and synchronizing user identifiers across Discover-Tech, Beeswax, Xandr, and Yandex. Once loaded on a website, the code stores user identifiers associated with Discover-Tech, Beeswax, and Xandr in the user's web browser in order to retrieve them again during subsequent visits to websites that load the same code.

The code is designed to initiate the ID syncing process by sending Discover-Tech's user identifier to Beeswax and Yandex in order to receive corresponding Beeswax and Yandex identifiers. Additionally, the code retrieves the user's Xandr identifier. Request chains archived on urlscan show Discover-Tech's tracking pixel in operation, including ID syncing with Yandex and the retrieval of user identifiers from Beeswax and Xandr.

When the tracking pixel code detects that a website visitor is located in a region where the GDPR applies, based on geolocating the user's IP address, it uses IAB Europe's Transparency and Consent Framework (TCF) to process user "consent" signals for the three TCF vendors Discover-Tech Ltd, Xandr Inc, and BeeswaxIO Corporation. This demonstrates how Discover-Tech utilizes its listing as a registered and approved ad vendor by IAB Europe, as discussed in Section 9.

The code also clearly maps the acronym "ZUID" to Xandr's user identifier. As detailed in Section 4, several Controlium modules refer to an option labeled "Detect ZUID". We are unsure how Discover-Tech's Controlium platform exactly utilizes this identifier. As the "Detect ZUID" option is among a few "Add Ons" that can be activated when setting up an ad campaign, it may serve the retrieval of Xandr user identifiers either for ad targeting or for tracking targets. Xandr (Microsoft Advertising) did not respond to our request for comment within the timeline provided.

Generally, the purpose of Discover-Tech's tracking pixel is unclear. As a large share of Discover-Tech ads are designed to lead users to the site myipinfo[.]io when clicking on those ads, the tracking pixel loaded during the site visit then correlates a target's Discover-Tech user identifier with their Beeswax, Xandr, and Yandex identifiers.

Records archived on urlscan show that the MyIPInfo website loaded a version of the tracking pixel from another domain associated with Discover-Tech in the past:

```
js.cookie-sync.xyz/myipinfo/c_tracking_pixel_gdpr.js
```

7. Discover-Tech and Its Corporate Network

Discover-Tech has been deeply embedded and interconnected with the digital advertising industry for years. In this section, we further investigate Discover-Tech, key persons affiliated with the company, related companies, and the origins of its MyDSP advertising technology.

Adtech with a Background in Spytech

Discover-Tech purports to be a typical digital advertising firm, offering a so-called Demand-Side Platform (DSP), which facilitates the delivery of targeted ads. On its website, it claims to have "unrestricted access to top-ranking apps with 1+ billion daily active users" via a "worldwide ad exchange". In addition

to its DSP, Discover-Tech offers "monetization" solutions to mobile network operators and mobile device manufacturers, which we discuss further below.

Israeli company records we reviewed link Discover-Tech's website, `discover-tech[.]io`, to the company Discover-Tech Ltd registered in March 2020, with Dekel Boni listed as its initial director and sole shareholder. In the two months after its incorporation, Eric Banoun, who is a major figure in the Israeli surveillance technology industry, joined Discover-Tech's board of directors, and the shareholder base was expanded. From April 2020, the company's shareholders included Dekel Boni, Guy Lants, Yaniv Basil, Zfanya Leib, Sergei Bartashevich, and Chaia Services Ltd, a company registered in the British Virgin Islands. Eric Banoun left the company's board of directors in January 2025 and Chaia Services Ltd ceased to be a shareholder in March 2026. As of July 2026, Discover-Tech is directed by Dekel Boni and owned by Boni, Basil, and Lants.

Eric Banoun co-founded the cyberespionage firm Circles, a close NSO Group affiliate, and Senpai Technologies, which is part of the Intellexa consortium. We could not access corporate registration information on Discover-Tech's shareholder Chaia Services Ltd. However, a Haaretz investigation reported that one of Chaia's directors was Sara Hamou. Hamou managed Intellexa's corporate network and was sentenced to eight years in prison (pending appeal) by a Greek court for her role in the Predatorgate scandal. Eric Banoun was listed as a director of a similarly named U.S.-based company, Chaia Services Tech LLC, which was dissolved in 2025.

Based on the links to Eric Banoun and Chaia Services Ltd., we conclude that Discover-Tech was linked to the spyware industry for almost six years, according to Israeli company records and other publicly available information.

Discover-Tech's other shareholders, including Dekel Boni who is now the company's sole director, have a background in digital advertising, previously working for adtech firms like Digital Turbine and Taptica, according to their LinkedIn profiles.[3] Boni lists himself as Discover-Tech's CEO, Guy Lants as its "Director of Product". Yaniv Basil lists himself as the company's "Chief Technology Officer" between 2020 and 2023.

Ad Vendor Registrations with Google and IAB Europe

Despite information about Discover-Tech's links to figures in the spyware industry that could be readily obtained from a review of corporate records, major advertising industry organizations added the company to several lists of "certified" or "approved" ad vendors, which helped make the company appear to be a legitimate advertising firm and facilitated its participation in the advertising ecosystem at scale.

[3] Accessed on June 17, 2026

As discussed in Section 9, Google listed Discover-Tech among its "Ad Manager Certified External Vendors", "Ad Technology Partners", and "Ads Personalization Providers" from 2020 until 2026. The advertising industry association IAB Europe listed the company on the "Global Vendor List" for its "Transparency & Consent Framework" (TCF), also from 2020 until 2026. In Section 9, we examine the implications of Discover-Tech's ad vendor registrations with Google and IAB Europe in detail.

Both the Google and IAB vendor registrations consistently refer to the Israeli company Discover-Tech Ltd and the domain `discover-tech[.]io`. In addition, Google's list of "Ads Personalization providers" clearly links Discover-Tech to the domains `mtrtb[.]com` and `mydsp[.]io`, which it listed among "domains which can be attributed to the provider" Discover-Tech Ltd.

Tracing the Origins of Discover-Tech's MyDSP Advertising Tech

As discussed in Section 5, the domain `mtrtb[.]com` and the ad system MyDSP (`mydsp[.]io`) play key roles in Discover-Tech's ad targeting.

According to historical whois information, Discover-Tech Ltd took ownership of both domains in 2020. While domain registration data became anonymized in 2022, `mydsp[.]io` redirected to `discover-tech[.]io` until early 2026. Both `mtrtb[.]com` and `mydsp[.]io` can be "attributed" to Discover-Tech Ltd according to Google, as discussed in Section 9.

MyDSP was launched by the Israeli adtech firm Matomy in 2016. In 2018, MyDSP was "connected" to Matomy's MobFox subsidiary, had "access" to 50 billion daily ad impressions and was able to target 500 million users, according to its website. Also in 2018, Matomy sold MyDSP to the Cypriot firm Marketcom Technologies Ltd, which belongs to the e-commerce firm Market Group owned by the Israeli billionaire Teddy Sagi, as confirmed by public filings, business data, media reporting, and whois information for the domains `mydsp[.]io` and `mtrtb[.]com`. A 2019 version of the `mydsp[.]io` site confirms that MyDSP ultimately became part of Glispa, a Berlin-based adtech firm also acquired by Market Group back in 2015.

We are not aware of any robust information that shows how Discover-Tech Ltd eventually took over MyDSP, but whois information confirms that Discover-Tech Ltd, founded in March 2020, took control of the domains `mydsp[.]io` and `mtrtb[.]com` from Marketcom Technologies Ltd at some point between June and October 2020. According to a Google record, the ad provider with the ID '3036' changed from MarketDSP (`advertising.market[.]com`) to "Discover-Tech Ltd" (`discover-tech[.]io`) on July 31, 2020. While the company names and websites changed, the list of additional domains attributable to this Google ad provider stayed identical: (`mydsp[.]io` and `mtrtb[.]com`).

JavaScript code related to MyDSP's admin interface for customers, published on admin.mtrtb[.]com, details a list of ad vendors MyDSP was connected to at an unspecified point in time (archived code). The list includes Google, Yandex, Vungle, and Sunteng. Thus, it confirms the connections with the ad vendors we found in Discover-Tech's bidding records (Section 5). In addition, the list suggests that MyDSP was or

is also connected to the ad vendors MobFox, Inneractive, MoPub, PulsePoint, RhythmOne, GumGum, Pubmatic, Smaato, Sonobi, NativeAds, Unity, Q1Media, and Applovin.

Offerings for Mobile Carriers and Device Vendors

Discover-Tech Ltd itself can be traced back to a company named RelevanTech Ltd (`relevantech[.]com`), founded by Discover-Tech shareholders Dekel Boni and Yaniv Basil in 2015, according to their LinkedIn profiles and Israeli company records we reviewed. Like MyDSP, RelevanTech was also acquired by Market Group's Glispa in 2017, and became Glispa Discover. Boni and Basil then worked for Glispa, before creating Discover-Tech Ltd in 2020.
The descriptions of the services provided by RelevanTech (2016), Glispa Discover (2017), and Discover-Tech Ltd are very similar. The current `discover-tech.io` site promises to help mobile network operators and mobile device manufacturers benefit from "sponsored and tailored app recommendations," in addition to the company's DSP offering. The 2022 version of the site explained that Discover-Tech would "place" mobile apps on new mobile devices "from the moment" they are "turned on" and provide "operator certified installs" of apps on new devices.

We are not aware of any robust information that shows how Discover-Tech's founders regained control over what was left of RelevanTech from Glispa, but whois information confirms that Discover-Tech Ltd regained control of the domain `relevantech[.]com` in July 2020.

In 2021, Discover-Tech Ltd operated a mobile app on behalf of the Serbian subsidiary of the mobile network operator A1 Telekom Austria, according to a terms of use agreement, which explains that the app would provide A1 customers with content from both A1 and Discover-Tech. The description on the 2021 version of the Serbian A1 website suggests that the app, named "Moy A1" ("My A1"), enabled A1 customers to check their mobile plan, download invoices, and buy additional credits. Put differently, Discover-Tech was sitting inside the official app of the third-largest Serbian mobile operator. We do not know for how long Discover-Tech was involved in operating this app.

The 2020 version of the Discover-Tech lists A1 and device manufacturers like Samsung, Tecno, and Wiko among the company's customers. We did not further investigate Discover-Tech's mobile carrier and device manufacturer business, which may or may not be active anymore.

In conclusion, we believe that Discover-Tech emerged from both RelevanTech and MyDSP, both previously owned by Glispa. While MyDSP and additional software for the delivery of malicious ads appear to be operational in 2026, an asset sale discussed in the next subsection suggests that Discover-Tech may not offer its services for mobile carriers and device manufacturers anymore.

A Sale of Assets Leaves Open Questions

In 2021, the Dubai-based firm Affle MEA FZ-LLC, part of the mobile advertising group Affle, based in Singapore and India, acquired "business assets" from Discover-Tech Ltd, according to public filings.

Publicly available financial statements refer to the acquisition of a Discover-Tech "business segment" including "brand, IP, domain, business relationships and goodwill."

Public filings further specify that Affle acquired Discover-Tech's "mobile device marketing platform" that provides "initial device customization" including "dynamic app discovery and recommendation at initial boot or reset of a device" through its integrations with device manufacturers and mobile network operators. An Affle press release quotes Discover-Tech founder Dekel Boni stating that he was "proud" that Discover-Tech's "technology" that "powers the first interaction a user has with his new device" would become part of the "app discover offering" of Appnext, another company acquired by Affle.

Based on the information available to us, we believe that Discover-Tech Ltd sold its offerings for mobile carriers and device vendors examined in the previous subsection, to Affle. We have no reason to believe that Affle has any control over Discover-Tech's malicious ad operations that we investigate in this report. However, the exact scope of this asset sale remains unknown to us. Affle did not respond to our request for comment within the timeline provided.

Links to Intelos and Other Websites

In a parallel investigation, the ad security firm Confiant found that the websites `discover-tech[.]io` and `tekma-dmp[.]ai` were published from a single user account using the website publication system Wix, which embeds the customer "userid" in each site's page metadata.

Additionally, we found that the website `discover-tech[.]io` has been sharing a single Wix user account with the website `intelos[.]io` for years. At some point after February 2026, the site `intelos[.]io` switched to a different "userid". This switch strongly suggests that the websites `discover-tech[.]io` and `intelos[.]io` have been published by the same entity from at least September 2023 until February 2026.

As detailed in Section 8, the mercenary ADINT vendor Intelos, which reportedly offers both ad-based geolocation surveillance and the delivery of spyware via ads, has additional links to Discover-Tech via Intelos shareholder Eric Banoun (2018 – present), who was also a director of Discover-Tech (2020 – 2025).

As **Table 8** shows, the Discover-Tech website shares the Wix user account with additional sites linked to Akedo (see the next subsections) and Tekma (see Section 8).

Website	**Wix userId: "a620bcc2-0237-4cbc-94c2-219ab49bed45"**
www.discover-tech.io	Sep 2023 – Oct 2026
www.intelos.io	Dec 2022 – Feb 2026

www.tekma-dmp.ai	Apr 2024 – Oct 2026
www.tekma.io	Mar 2022
www.partners.akedo.gg	Apr 2024 – Oct 2026

Table 8: Wix "userid" overlaps across Discover-Tech, Intelos, Tekma, and Akedo.

Adtimizer

We observed Discover-Tech using the domain `dtech.adtimizer[.]co` as impression and click URLs in ads. Israeli company records link the domain `adtimizer[.]co` to the Israeli firm Adtimizer Ltd, directed and owned by Oren Baranes. Baranes also appears in the HTML source code of the Controlium platform on the sites `www.controlium[.]net` and `powerium[.]net`:

```
<meta name="google-signin-client_id"
content="oren.baranes@discover-tech.io.apps.googleusercontent.com">
```

Furthermore, three users, "Oren Baranes", "Oren baranes" (lowercase B), and "Oren Baranes Admin" regularly logged into Controlium in July 2026, according to authentication logs reviewed by us (see Section 3).

In 2022, Baranes posted on a public web forum[4] using a Discover-Tech email address, in a forum thread that was discussing the advertising firm Beeswax:

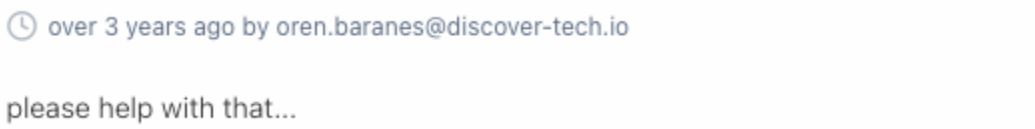


Figure 24: Baranes' post on a public web forum using a Discover-Tech email address.

Baranes' LinkedIn profile does not mention Discover-Tech but presents him as an expert in mobile advertising.[5] His appearance in the Controlium source code and his email address, which are both clearly linked to Discover-Tech, suggest that Oren Baranes is working for the company in some capacity. We consider the domain `adtimizer[.]co` and the Israeli company Adtimizer Ltd as linked to

[4] Not available on the web anymore, but archived by the authors of this report on 18.8.2025: https://api-docs.freewheel.tv/advertiser/v2.0/discuss/60a53c1531fb4d001c01435e

[5] Accessed on June 17, 2026

Discover-Tech. However, we do not have conclusive evidence that Adtimizer Ltd knowingly participated in the delivery of mercenary spyware attacks.

In its response to the Citizen Lab, Adtimizer Ltd claims that the subdomains we consider to be linked to Discover-Tech, including `dtech.adtimizer[.]co`, `myinfoback.adtimizer[.]co`, `noas.adtimizer[.]co` and `tekma.adtimizer[.]co`, were "used solely within Discover Tech's infrastructure, which was entirely separate from ours and was not operated, managed, or controlled by Adtimizer", and that Adtimizer "had no knowledge of, or involvement in the alleged activities" with respect to Discover-Tech's malicious ad targeting.

MyIPInfo, Akedo, and Volasim

As discussed in Section 4, the sites `adv45.volasim[.]com` and `adv50.volasim[.]com` provided versions of Discover-Tech's Controlium platform. The site `myipinfo[.]io` hosts a decryption tool linked to Controlium including keys used in conjunction with the Candiru attacks. The bidding logs reviewed in Section 5 show that the vast majority of ads served via Discover-Tech promote the MyIPInfo site, the mobile gaming platform Akedo, and an app provided by Volasim.

The following subsections show that MyIPInfo, Akedo, and Volasim are linked to Discover-Tech and to each other in additional ways. The subsection 'Response from Volasim Ltd' below addresses in more detail Volasim's response to The Citizen Lab where the company emphasizes that it has "no involvement whatsoever" in "spyware-related activities."

Akedo

Akedo's management team includes two Discover-Tech key executives and shareholders, Dekel Boni and Yaniv Basil, according to a promotional pdf published on the company's website, `akedo[.]gg`. A person named Kfir Goldman is listed as the general manager of the Akedo platform. The document was created by a person, who is the "Chief Marketing Officer" at both Akedo (since 2022) and Discover-Tech (since 2019), according to their LinkedIn. Another person refers to themselves as the "Operations Manager" at both Akedo (since 2022) and Discover-Tech (since 2023). The fact that two persons work at both Akedo and Discover-Tech at the same time and in the same role, combined with the overlaps in the management team, indicates a relationship between the two companies.

The Akedo site does not refer to any legal entity. Israeli company records reviewed by us indicate that Eric Banoun, Dekel Boni, Yaniv Basil, and Kfir Goldman were shareholders in a firm named KYD Ltd, which in turn was a shareholder in a company named "Akedo Good Game Ltd", which was directed by Boni. The two companies were dissolved in 2024 and 2025. As both the website and the Israeli company records refer to the same group of persons, we believe that the two legal entities were linked to Akedo's activities until their dissolution.

Kfir Goldman, who is listed as part of Akedo's management team and who was an indirect shareholder in Akedo Good Game Ltd, is included in a list of user accounts we found in the source code of Discover-Tech's "Mini Platform C" app, as examined in Section 3. The listed accounts also include Dekel Boni, Yaniv Basil, and Guy Lants. This suggests that Kfir Goldman is or was also working for Discover-Tech in some capacity.

Volasim

The website `volasim[.]com` describes Volasim as a "digital marketing agency," incorporated in Cyprus as Volasim Ltd, which serves advertisers using "ad platforms and real-time bidding platforms". The address mentioned on the website and the registration address of Volasim Ltd, according to company records from Cyprus, are identical. The company is directed and owned by a person who is listed as a director of many companies registered in Cyprus, likely on behalf of other parties. We were not able to access information about Volasim's ultimate beneficial owners.

Volasim Ltd is listed as a mobile app developer by both Google and Apple. It provides the game City Masters, the reminder app RemindMeWhere and two apps named MyIPInfo and Akedo. All four app listing pages refer to Volasim Ltd as the developer of the app, using the same address as mentioned in the corporate record and on the Volasim website. The app listing page for MyIPInfo refers to the website `myipinfo[.]io`, the page for the Akedo app refers to the site `akedo[.]gg`. The page for Volasim's game lists the support email address `kfir@volasim[.]com`. We are not aware of any information confirming that this email address is associated with Kfir Goldman.

In addition to Discover-Tech's Controlium platform being available on the sites `adv45.volasim[.]com` and `adv50.volasim[.]com`, the Controlium source code contains example data for the creation of a banner ad campaign for Volasim's RemindMeWhere app, with the ad linking to the app's website, `remindmewhere[.]app`. A Controlium-related "Banner Tester" app, as examined in Section 3, contains the description "Volasim test banner" in the source code. We also found a YouTube channel named "DT_VLSM" that uses Discover-Tech's logo and lists a video that advertises Volasim's reminder app.

MyIPInfo

The site `myipinfo[.]io` hosts Controlium-related code and is often being advertised by Discover-Tech. In addition, we found the same Google Tag Manager ID, which identifies a specific Google customer and their third-party tracking configuration across the sites `myipinfo[.]io` and `events-ui.discover-tech[.]io`, based on source code analysis. Passive DNS data indicates that the domain qabackend.myipinfo.io was linked to `ipinfo.myweb3id.io`. Several subdomains of `myweb3id[.]io` provide Controlium-related code and NOAS services, as discussed in other sections of this report.

The website `myipinfo[.]io` predominantly displays ads for Akedo, according to browser testing and the observation that the site loads a file named "ads.json" that contains Akedo ad data (urlscan). Based

on source code analysis and data from the analysis tool DNSlytics, we found the same Google AdSense ID, which identifies a specific publisher selling ads via Google, across the sites `events-ui.discover-tech[.]io`, `myipinfo[.]io`, and `akedo[.]gg`. Another AdSense ID has been observed across the sites `myipinfo[.]io`, `akedo[.]gg`, and `citymaster[.]io`, which is the website for Volasim's game app "City Masters".

Response from Volasim Ltd.

In its response to the Citizen Lab, Volasim Ltd refers to "Akedo" and "MyIPInfo" as "legitimate digital products developed by Volasim". The company states that Discover-Tech was among the "external advertising providers" it engaged to "promote its products". Volasim emphasizes in its response that it "has no involvement whatsoever in the spyware-related activities" discussed in our investigation, and that it has "never commissioned, authorized, participated in, or knowingly facilitated any such activity". As summarized in this subsection ('MyIPInfo, Akedo, and Volasim'), we found that Volasim and its products Akedo and MyIPInfo are linked to Discover-Tech in several ways. However, at this time, we do not have conclusive evidence that Volasim Ltd knowingly participated in the delivery of mercenary spyware attacks.

8. Intelos, Bindecy, and Candiru's Corporate Networks

This section provides an overview of Intelos, Bindecy, and Candiru, and provides details on what we know about their corporate networks and business identities. Furthermore, we present additional links between Discover-Tech and Intelos.

Intelos and its ADINT System AdHoc

In 2023, the trade press website Intelligence Online and Haaretz first reported about Intelos, a new Israeli ADINT vendor that provides a surveillance system based on data from digital advertising named "AdHoc". Intelos was reportedly founded by Eric Banoun, who is "one of the pioneers of offensive cyber in Israel" according to Haaretz. Israeli company records reviewed by us confirm that Banoun has been a shareholder in Intelos Ltd from its registration in 2018 until present, and he is listed as the company's director. The email address he uses in corporate filings, `eric@intelos.io`, clearly links Intelos Ltd to the website intelos.io.

The fact that Banoun was also listed as a director of Discover-Tech Ltd (see Section 7), already suggests a potential connection between the ADINT vendor Intelos and Discover-Tech. In addition, the websites `intelos[.]io` and `discover-tech[.]io` were published by the same entity until at least February 2026, according to technical analysis discussed in Section 7. While we cannot assess the exact scope of the collaboration between Intelos and Discover-Tech, the technical analysis discussed in Section 4 indicates that the two work together.

Besides a few media articles and the company's website, there is almost no public information available about Intelos. The company's AdHoc product is not mentioned on its website. According to Israeli company records reviewed by us, Intelos Ltd's shareholders include Eric Banoun, Senpai co-founder Roy Shloman, Thai businessman Charoenrath Vilailuck, and a Liechtenstein-based firm named SAR Investments International Ltd, among others.

On its website, Intelos purports to be a "marketing intelligence" platform that monitors "worldwide digital signals, actions, and preferences", including "subtle changes in behaviour", by processing 16 billion "daily data sets" across 50 countries. Much of the promotional language on the site sounds like the company's products are built for customers in digital marketing, but could also describe an ADINT vendor. Intelos promises to "map behavioural patterns across audiences" and to build "profiles of audiences and groups" in order to "map relationships, track behavioural shifts, and anticipate collective action". It also provides "location intelligence" based on a "proprietary index of the physical world" with "every relevant location classified, mapped, and weighted for significance". Another system named "Nexus AI" could transform "raw data into structured insights" based on "live and historical datasets" in order to "map behavioural clusters" and "detect relationships".

Haaretz and Intelligence Online reported that Intelos provides ad-based geolocation surveillance but also the delivery of spyware via ads, without providing details about the latter. Its technology was reportedly offered to the Shin Bet in Israel and sold in Thailand. According to Haaretz, Eric Banoun presented an ADINT product named "Havoc" that included the AdHoc logo to an Egyptian customer. An agreement related to his presentation mentioned a U.K. firm, whose director is also the director of another U.K. firm named "Havoc", which sold an unnamed cyber system to an unnamed country over a period of three years at a cost of about $42 million. Based on the media report, it remains unclear whether AdHoc was sold in Egypt or not.

Intelos did not respond to our request for comment within the timeline provided.

Tekma

The 2025 version of the site `intelos[.]io` shares many promotional phrases with the 2024 version of the website `tekma-dmp[.]ai`. Both sites offered a "Data Marketing (DM) platform" and the "AI Edge" product using a number of identical sentences. According to the current website, Tekma purports to have access to data on 3.5 billion devices, which can be utilized "across major DSPs", and is based in Dubai, with regional offices in Greece, Cyprus, and Spain. The 2024 site includes Tekma contact information referring to "Chaia Services" and mentions another regional office in Hong Kong. Another older but also almost identical site, `tekma[.]io`, includes Tekma contact information referring to "Chaia Ltd" in "13&15 GR. Afxentiou Street, Mesa Geitonia Limassol, Limassol 4003 CY".

Technical analysis discussed in Section 7 shows that the websites `intelos[.]io`, `tekma-dmp[.]ai`, `discover-tech[.]io`, and `www.partners.akedo[.]gg` were published by a single entity between 2024 and 2026. The site `tekma[.]io` was also published by the same entity.

As discussed in Section 7, Discover-Tech Ltd's shareholders include a company named Chaia Services Ltd. Notably, the Israeli firm Adtimizer Ltd (see Section 7) has the subdomain `tekma.adtimizer[.]co`. Between 2020 and 2025, this subdomain was linked to the following host name via CNAME, according to DNS telemetry:

```
discovertech-alb-100966113.us-east-1.elb.amazonaws.com
```

Discover-Tech Mercenary Spyware Partner: Bindecy

Bindecy is "one [of] Israel's lesser known spyware firms", though it "develops and sells digital surveillance tools to states" with a focus on "Western clients and their close allies in the east", according to Haaretz. On its website, bindecy.com, it presents itself as a cybersecurity firm founded by Israeli military intelligence alumni that analyzes apps and "critical systems". The trade press website Intelligence Online reported that Bindecy, founded by Daniel Shapiro and Eylon Ben Yaakov, has "cyber offensive contracts from the Israeli intelligence services" and sold its "zero-click spyware" to Italy's military police, the Carabinieri.

In 2021, Bindecy acquired part of the intellectual property of Merlinx, another Israeli cyber offensive company formerly known as Equus Technologies. In 2024, Haaretz reported that the founders of Bindecy recently joined the Spanish company Epsilon, which develops exploits and is "aiming for the American market", as partners. According to its website, `epsilon-sec.com`, the company offers security research on mobile platforms and is located in Spain, France, and Canada.

Company records reviewed by us indicate that the Israeli company Bindecy Ltd was founded in 2017. Since 2025, it has a solely owned subsidiary named Shor Labs s.r.o. registered in the Czech Republic. Bindecy co-founder Daniel Shapiro is listed as a director of both Shor Labs s.r.o and Spanish Epsilon Cyber SL.

Bindecy did not respond to our request for comment within the timeline provided.

Discover-Tech Mercenary Spyware Partner: Candiru/Integrity Labs

Candiru is an Israeli-founded mercenary spyware company that draws its original name from the parasitic Candiru fish, and has operated under a wide range of names throughout the years, including Saito Tech. Today, Candiru operates under the rebranded identity of Integrity Labs after acquisition by U.S.-based Integrity Partners.

Candiru: Prior Investigations, Abuses, and Discoveries

Candiru is a mercenary spyware threat actor known by multiple names, including SOURGUM and Carmel Tsunami by Microsoft.

First Candiru Abuse Discoveries: 2021

On July 15, 2021, the Citizen Lab published the first report exposing Candiru. That investigation included identifying a Candiru victim and recovering a copy of Candiru's Windows spyware. We then worked with Microsoft's Threat Intelligence Center (MSTIC) to analyze the spyware, which led to the identification of two zero-day vulnerabilities (CVE-2021-31979 and CVE-2021-33771). We also identified over 750 websites linked to Candiru's infection infrastructure that masqueraded as a wide range of civil society entities ranging from media organizations to Amnesty International.

On July 14, 2021, Google TAG published a report which included discussion of two Chrome exploits (CVE-2021-21166 and CVE-2021-30551) that pointed to addresses matching our Candiru fingerprint. The report also linked a Microsoft Office exploit (CVE-2021-33742) to the same operator.

Microsoft's own investigation into Candiru, published simultaneously with our report on July 15, 2021, identified at least 100 spyware victims across ten countries. Microsoft reported that the victims included journalists, opposition politicians, dissidents, and activists.

On November 16, 2021, ESET reported on a series of watering hole attacks observed in 2020 and 2021 targeting websites in the Middle East with what they described as a "strong focus on Yemen." They attributed the attacks to Candiru.

Further Investigations and Abuses: 2022-2025

In 2022, the Citizen Lab again found Candiru spyware targeting victims among Catalan civil society groups in Spain. In that investigation, we identified signs of a live Candiru infection on a Catalan university network, and successfully worked with system administrators to identify the victim, isolate the device, and extract the active spyware. The targeting we observed as part of this campaign included emails masquerading as official Spanish governmental messages about COVID.

On July 21, 2022, Avast published a report revealing that Candiru was using a Chrome zero-day exploiting WebRTC (CVE-2022-2294), and found evidence of targeting of users in multiple countries in the Middle East.

On December 22, 2022, Meta disclosed that it disrupted around 130 Facebook and Instagram accounts used by Candiru to send infection links amongst themselves to "test phishing capabilities."
In the summer of 2024, during the parliamentary election campaign, Member of the European Parliament (MEP) Daniel Freund was targeted with Candiru's mercenary spyware, according to the European Parliament's security services.

On August 5, 2025, Recorded Future's Insikt Group investigated Candiru infrastructure and identified multiple Candiru clusters linked to Hungary, Saudi Arabia, Indonesia, and Azerbaijan, among others.

On September 2, 2025, Sekoia published an investigation into Candiru's spyware, highlighting how Candiru and similar companies leverage complex jurisdictional structures to avoid discovery.

Entity Listing

On November 3, 2021, Candiru was added to the United States Commerce Department's Entity List for malicious cyber activities. The entity listing noted that Candiru was added because "they developed and supplied spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers."

Legal Actions Against Candiru and Users

In October 2024, Daniel Freund filed a criminal complaint with the assistance of German digital rights NGO GFF against Viktor Orbán and unnamed persons over his targeting with Candiru.

On April 30, 2025, the NGO Sentinel Alliance filed a case against multiple Spanish governmental entities, NSO Group, and Candiru over the mercenary spyware attacks targeting Catalan civil society.

Candiru's 2025 Acquisition by Integrity Partners

In April 2025, Israeli media reported that U.S.-based Integrity Partners acquired the operations of Candiru for $30 million in a bid to bypass the U.S. Entity Listing. Research by Recorded Future's Insikt Group identified Candiru as having been rebranded to "Integrity Labs" (אינטגריטי לאבס בע~מ) in December 2024. The current status of the acquisition is unclear.

Candiru/Integrity Labs did not respond to our request for comment within the timeline provided.

9. Discover-Tech's Relationship to the Digital Advertising Industry

This section explores how major industry organizations and ad vendors helped enable Discover-Tech's ad operations, and notes that Discover-Tech achieved "certified" and "approved" status by Google and the major advertising industry association IAB Europe.

Our analysis indicates that Discover-Tech deployed ads via Google, Yandex, and other ad vendors including Beeswax (FreeWheel/Comcast), Vungle (Liftoff), Eskimi, and Sunteng. In addition, both Google and the advertising association IAB Europe have listed Discover-Tech as a "certified" and "approved" ad vendor since the year 2020, which helped make the company appear to be a legitimate advertising firm and facilitate its participation in the advertising ecosystem at scale.

As a result of this investigation, both Google and IAB Europe removed Discover-Tech from their ad vendor registries in early October 2026. Google, which collaborated in the investigation, terminated Discover-Tech's access to its ad exchange platforms. Beeswax removed Discover-Tech from its ad buying

platform. Vungle (Liftoff) paused Discover-Tech's access while conducting a review. Eskimi blocked Discover-Tech's accounts and domains.
The ad vendors identified in this section are distinct from mercenary spyware or ADINT vendors insofar as they are not necessarily aware of potential misuses of their infrastructure for non-advertising purposes.

Discover-Tech: Got "Certified" and "Approved" by Google and IAB Europe

Table 9 provides an overview of ad vendor lists maintained by Google and IAB Europe, the European branch of the major advertising industry association IAB, which included Discover-Tech from the year 2020 until early October 2026:

	Ad Vendor List	Discover-Tech Entry/Vendor Metadata	Listing
IAB Europe	Transparency & Consent Framework (TCF), Global Vendor List (GVL), available in JSON format (vendor-list.json)	– Vendor ID: 778 – Name: Discover-Tech ltd – Privacy Policy: discover-tech.io/privacy-policy – Disclosure info: discover-tech.io/_functions/api/disclosure.json	2020-07-02 (vendor-list.json) to 2026-10-08
Google	EU Ad Technology Providers for Ad Manager, AdSense, AdMob, Display & Video 360	– Name: Discover-Tech LTD – Privacy Policy: discover-tech.io/dsp-privacy-policy – Vendor ID: 4824 – Name: Discover-Tech LTD – Vendor type: Demand Side Platform – Privacy policy: discover-tech.io/dsp – Can access Google Display Network (GDN): Yes – Needs to be declared: No	2020-08-12 to early Oct 2026 2020-11-01 to early Oct 2026
Google	Ad Manager Certified External Vendors	– Vendor ID: 4824 – Name: Discover-Tech LTD – Vendor type: Demand Side Platform – Privacy policy: discover-tech.io/dsp – Can access Google Display Network (GDN): Yes – Needs to be declared: No	2020-11-01 to early Oct 2026
Google	Ads personalization providers, available in CSV format (providers.csv)	– Provider ID: 3036 – Name: Discover-Tech LTD – Privacy Policy: discover-tech.io/dsp-privacy-policy – Provider domains: mtrtb.com, mydsp.io, tracker.mtrtb.com	2023-10-10 (providers.csv) to early Oct 2026

Google	Google Authorized Buyers, What's New in RTB dictionaries	– "The providers.csv dictionary file has changed" – Deleted line 3036,"MarketDSP","https://advertising.market.com/dsp-privacy-policy/","mtrtb.com mydsp.io tracker.mtrtb.com" – Added line 3036,"Discover-Tech LTD","http://discover-tech.io/dsp-privacy-policy/","mtrtb.com mydsp.io tracker.mtrtb.com"	2020-07-31

Table 9: Discover-Tech in ad vendor lists maintained by Google and IAB Europe.

Google listed Discover-Tech Ltd among its roughly 2,400 Certified External Vendors. These vendors, which Google also refers to as "allowed vendors" and "certified companies", "undergo a business review," the nature of which is not specified, so they "can serve third-party ads on the Google Ad Manager platform". Google claims to "conduct a thorough certification process" for "vendors that are certified for third-party ads" and ensure they "meet Google's requirements for third-party ad serving". A listed vendor is "permitted to make third-party calls", which may include tracking pixels. Google emphasizes that it might pause the delivery of ads when it detects "non certified vendors". Being listed is crucial for a company that wants to interface with Google.

Google also listed Discover-Tech among its roughly 1,000 Ad Technology Providers, who can receive data on website visitors and app users in Europe. In Google's own words, these vendors "agreed to comply" with its "data usage policy" and "have shared certain information that is required by European regulations policy". Website and app publishers "need to list these partners for [their] users." Until 2025, Google referred to these vendors as "certified ad technology providers," but a later redesign of the page dropped the term "certified." In addition, Google listed Discover-Tech in its global list of roughly 1,700 ads personalization providers, which may participate in ad auctions based on "user consent". The list contains "domains which can be attributed to the provider." For Discover-Tech Ltd, the domains `mtrtb[.]com` and `mydsp[.]io` are listed.

Discover-Tech Ltd was added to all these lists in 2020. Google, which collaborated in this investigation, removed Discover-Tech from its ad vendor registries and terminated the company's access to its ad exchange platforms as of the first week of October, 2026.

Discover-Tech Ltd was also listed in the Global Vendor List (GVL) maintained by the European branch of the Interactive Advertising Bureau (IAB), a key digital advertising industry association. The GVL contains roughly 1,000 vendors that are "registered and approved" by IAB Europe. These vendors can participate in IAB Europe's "Transparency & Consent Framework" (TCF), which promises to enable ad vendors to comply with European data protection and privacy law when processing personal data for digital advertising purposes. While the TCF's ability to enable lawful data processing is controversially debated,

a GVL registration has become a de-facto requirement for an ad vendor to participate in digital advertising, display ads and receive data in Europe. IAB Europe added Discover-Tech Ltd to the GVL on July 2, 2020. As a result of this investigation, Discover-Tech was removed from the GVL on October 8, 2026.

According to IAB Europe, it takes "reasonable steps to vet and approve" vendor applications, including the "identity of the party or parties controlling the vendor" and the vendor's ability to "adhere" to a number of TCF policies, and then monitors their compliance with those policies. The TCF is the basis for passing user "consent" signals for personal data processing across the digital advertising supply chain, from users to publishers to intermediaries (like SSPs, DSPs, and ad exchanges) to advertisers, including in bid requests and tracking pixels. Most ad tags and tracking pixels that connect to third-party vendors require "consent" signals, including in some jurisdictions outside Europe and the U.K. like California. Google, Xandr, and most larger ad platforms require TCF compliance. While several studies found that vendors are too often ignoring "consent" signals, an ad vendor that is not listed in the GVL, and thus cannot pass any signal, can hardly interface with other ad vendors in reliable ways.

While the vendor lists maintained by Google and the IAB Europe help a company appear to be a legitimate ad vendor and are the basis to participate in the digital advertising ecosystem in a reliable way at scale, they appear to be largely based on self-attestation by vendors. They are also the basis for most of the "consent" popups shown to European web and app users every day. Discover-Tech Ltd's inclusion in those lists potentially means that, for almost six years, hundreds of millions of Europeans were presented with a consent request that, if the recipient clicked "Agree," could be construed as authorizing Discover-Tech to process their data under the GDPR.

As of October 2026, Discover-Tech is additionally listed in a registry operated by the "Trustworthy Accountability Group" (TAG) created by major U.S. advertising associations and the IAB, which aims to increase trust in the digital advertising industry, eliminate fraud and fight criminal activity including "malware threats targeting the digital advertising supply chain." The Verified by TAG badge held by Discover-Tech, which the company also displays on its website, is used across the industry to "determine trust and transparency" and let prospective partners know that a company has taken "actionable steps to verify their identities and adopt rigorous standards to fight online fraud, piracy, malware, and lack of transparency," according to the TAG website.

Advertising Firms Involved in Discover-Tech's Targeting

Our analysis of ad bidding data in Section 5 indicates that Discover-Tech targeted users by participating in ad auctions handled by Google, Yandex, and other ad vendors including Vungle and Sunteng. The analysis of the Controlium platform in Sections 3 and 6 indicates that Discover-Tech also uses the ad buying platforms Beeswax DSP and Eskimi DSP to target users. In addition, those sections show that Discover-Tech receives and utilizes user identifiers maintained by Microsoft's advertising platform Xandr.

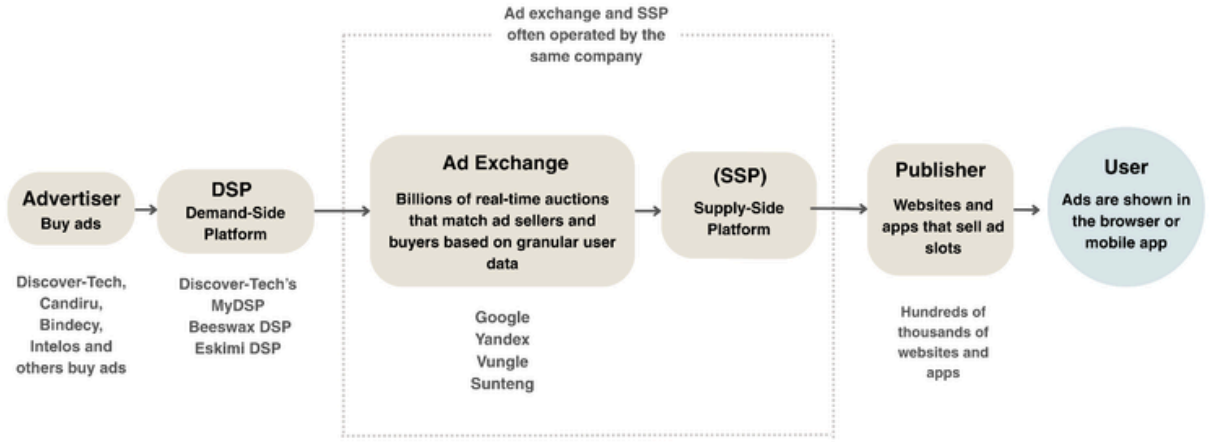


Figure 25: Vendors involved in Discover-Tech's ad operations across the advertising supply chain.

Table 10 provides a summary of ad vendors involved in Discover-Tech's ad operations, according to the research presented in this report. The table briefly summarizes our findings with respect to their involvement. The descriptions of vendors and their offerings are based on additional research that is included in the Appendix of this report.

Ad vendor	Product offerings	Findings
Google (U.S.)	Dominates the digital advertising ecosystem in the U.S., Europe, and other regions, and operates a massive ad exchange and systems for ad sellers and buyers.	Discover-Tech Ltd. delivered ads via Google, according to ad bidding records, URL telemetry data and source code of a campaign management system reviewed by us.
Yandex (Russia)	Dominates the digital advertising ecosystem in Russia and some other regions, and operates an ad exchange and systems for ad sellers and buyers.	Discover-Tech Ltd. delivered ads via Yandex, according to ad bidding records, URL telemetry data and source code of a campaign management system reviewed by us.

Beeswax, owned by Comcast's ad platform FreeWheel (U.S.)	Highly customizable DSP that allows clients to access granular bidding data and implement custom bidding algorithms ("bidder-as-a-service"), according to the company.	Discover-Tech used FreeWheel's Beeswax DSP to deliver ads and it appeared to use the Beeswax user identifier for targeting, according to URL telemetry data and source code from several systems operated by Discover-Tech reviewed by us. It also retrieved Beeswax user identifiers and engaged in ID syncing with Beeswax, according to browser testing, source code analysis, and records archived on the web investigation platform urlscan.
Eskimi (Lithuania)	DSP and white-label DSP, which allow clients to target 1.5 billion "profiled users" across 60 ad exchanges, according to the company.	Our analysis of Discover-Tech's Controlium platform indicates that the company used Eskimi as one of three DSPs for ad delivery. URL telemetry data reviewed by us confirms ad delivery via Eskimi DSP, albeit the volume is low compared to ads delivered via MyDSP and Beeswax.
Vungle, owned by Liftoff (U.S.)	Mobile SSP and ad exchange, both relying on the "Vungle SDK", which is embedded in 150,000 apps and used by one billion people, according to the company.	Discover-Tech delivered ads via Vungle, according to ad bidding data reviewed by us.
Sunteng, also known as Shunfei Technology (China)	DSP, SSP, and ad exchange, which processes 50 billion ad bid requests a day across 10,000 mobile apps and 60 ad vendor partners, according to the company. Corporate websites reviewed by us suggest that Sunteng is associated with BiddingX and Bidex.	Discover-Tech delivered ads via Sunteng, according to ad bidding data reviewed by us.
Xandr, aka Microsoft Advertising (U.S.)	Xandr, in 2023 rebranded Microsoft Advertising, offers a SSP and identity graph/syncing	Discover-Tech retrieved user identifiers from Xandr and engaged in ID syncing with the

	services. Its “Invest” DSP was shut down in early 2026.	vendor, according to browser testing and our analysis of source code and records archived on the web investigation platform urlscan. Discover-Tech’s Controlium platform provides an extra option to “detect” the Xandr user identifier.

Table 10: Ad vendors involved in Discover-Tech’s ad operations.

Google, which collaborated in the investigation, terminated Discover-Tech’s access to its ad exchange platforms in early October 2026. As detailed in their responses to the Citizen Lab, Beeswax removed Discover-Tech from its ad buying platform, Vungle (Liftoff) paused Discover-Tech’s access while conducting a review, and Eskimi blocked Discover-Tech’s accounts and domains. Sunteng and Xandr (Microsoft Advertising) did not respond to our requests for comment within the timeline provided.

10. Discussion: AdFection Shows That Online Ads Are a Cybersecurity and Privacy Crisis

This report provides the first-ever technical evidence of zero-click mercenary spyware attacks delivered via targeted advertising. We also confirm that AdFection was used to infect devices at international media organization Al Jazeera.

These attacks were facilitated by Discover-Tech, which presents itself as a legitimate advertising business but actually serves as a bridge between mercenary spyware companies and the advertising ecosystem. Discover-Tech not only helps companies like Candiru use ads to mass-profile unwitting phone users, their ads directly enable these companies to silently infect selected targets’ devices.

The combination of advertising intelligence and the delivery of spyware is extremely concerning, for several reasons. First, both the digital advertising and mercenary spyware industry are very poorly regulated, with the latter featuring numerous firms notorious for deception, a lack of transparency, and even unlawful activities. To see entities from those two industries forming an alliance should be a wakeup call to regulators and policymakers around the world. Dozens of reports by numerous organizations, including the Citizen Lab, have shown incontrovertible proof of the harms caused by mercenary spyware vendors on civil society around the globe. With the addition of the type of advertising intelligence capabilities we have documented, those firms’ capabilities will now be supercharged.

Second, the combination of advertising intelligence and spyware infections provide government security agencies with highly invasive systems that span both mass and highly targeted types of user surveillance. As we show in this report, millions of devices were likely unwittingly profiled as a form of preliminary reconnaissance to enable targeting with spyware tailored to those device's specific characteristics. Ominously, many of these infections took place without any visible indication of tampering or other clues that might have alerted them to the compromise. Also ominous is the fact that the services of Discover-Tech appear to span multiple regions around the globe. It is not known at this time exactly which governments are capitalizing on these new capabilities, but if past evidence is any indication it seems highly likely that some proportion of them are abusing those capabilities to target individuals outside of strictly criminal or national security purposes.

ADINT: Journalism in the Crosshairs

The hacking of Al Jazeera with AdFection is part of a longstanding pattern: mercenary spyware attacks against the media. Journalists and newsrooms are a constant target for spyware attacks, and this latest case highlights how well-resourced operators consistently seek new ways to access their private, protected communications.

The use of spyware to target the media directly interferes with the ability of the free press to hold power to account. It also threatens the privacy of journalists' sources, and can chill reporting. Foreknowledge of movements, reporting topics, meetings, and sources does not just help powerful interests try to frustrate coverage and reporting, it can put people at physical risk. This is especially true for a news organization with reporters, freelancers, stringers, fixers and sources working in conflict zones around the world.

Investigations into mercenary spyware operations have repeatedly surfaced targeting against the media, including in the context of governmental and cartel killings of reporters. Journalists have been confirmed spyware targets, from the Citizen Lab's earliest findings of Pegasus spyware in Mexico almost a decade ago, to cases across Africa from Angola to Morocco and Togo, to Jordan, Serbia, El Salvador, and Italy, among many others. Organizations like Reporters Without Borders provide helpful overviews of the scale of the threat which, as Access Now points out, is sometimes coupled with laws designed to authorize government access to journalists' communications. The International Federation of Journalists, meanwhile, has a recent overview of how spyware is situated within a broader set of digital threats against journalists.

Recently, reporting from the Committee to Protect Journalists outlined the dangers posed to journalists from ADINT-style tracking. The combination of this tracking with zero-click mercenary spyware targeting presents an even more serious danger to journalists' safety.

This investigation should also serve as a clear warning signal to news organizations around the world that they may be being actively targeted via this new threat. This targeting may happen both in newsrooms and to individual journalists, editors, and other staff members. We urge news organizations

to immediately seek expert assistance and ensure that their systems are protected against these attacks to the fullest extent possible. We provide some guidance in Section 11, however we urge all news organizations to systematically review their security posture (and logs) for signs of AdFection style spyware targeting and infection.

The Advertising Industry: A Dangerous Lack of Due Diligence

Our findings also reveal a troubling lack of due diligence within the digital advertising industry that helped enable this inappropriate activity. Discover-Tech, which presented itself as a legitimate ad vendor but served as a bridge between the online advertising ecosystem and the spyware industry, has been deeply embedded and interconnected with the online advertising ecosystem for years. Multiple ad vendors let the company utilize their systems. The two key industry organizations, Google and IAB Europe, have helped Discover-Tech appear as a legitimate ad vendor from the year 2020 until 2026, despite information about the company's links to figures in the spyware industry being readily accessible in corporate records. Our findings show that the digital advertising industry is ill-prepared to prevent malicious actors from exploiting its infrastructure for the distribution of spyware via targeted ads.

Advertising Industry: Prioritize Security, Stop AdFection

This case should serve as an alarm to the advertising industry that business as usual is no longer acceptable. The online advertising industry must get serious about tackling the distribution of mercenary spyware via targeted ads, alongside other malicious advertising practices including financially motivated fraud and cybercrime. Technical and organizational measures currently implemented by the industry, such as the SafeFrame specification or standards for supply chain transparency are insufficient or not even adopted in a meaningful way.

Fix a Broken Digital Infrastructure

More broadly, the distribution of spyware via targeted ads depends on the way digital advertising – and the web economy at large – currently operate.

Many mobile apps and websites contain tracking software operated by dozens of third parties, which themselves may include code by additional third parties within apps and browsers. Also required for the targeted deployment of spyware, ad targeting at the individual level depends on uncontrolled data sharing via RTB auctions and third-party tracking.

Automated ad selling and buying via RTB, which connects large numbers of publishers, advertisers and intermediaries across opaque supply chains, is designed to minimize human intervention. When combined with a lack of oversight and accountability, it is generally prone to abuse. This is further aggravated by the assumption that at least some ad vendors benefit from malicious and fraudulent advertising. Leaked internal documents from Meta reported by Reuters suggest that Meta estimated that

it earns between five and ten percent of its annual revenue from running fraudulent ads. Industry sources suggest that ad fraud accounts for one fifth of all online advertising spend.

This broken digital infrastructure needs to be reformed at several levels, as consumer associations, regulators, and policymakers have long been demanding.

AdFection: A Threat to States, Civil Society, and Everyone Else

The distribution of spyware via targeted ads represents a security risk not only for potential victims but also for states and civil society at large. Two major U.S. security agencies, the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA), have warned already in 2018 and 2020 that adversaries may leverage malicious ads to deploy malware on devices, and thus both recommended that government agencies and other organizations use ad-blocking software.

Given the current threat posed by Discover-Tech's AdFection vectors, and the evidence of wide-scale targeting, we judge that the most feasible protection is for defenders to block targeted ads at the gateway. This defensive recommendation (see Section 11) holds until the industry has shown that it is reliably able to block all AdFection style vectors.

At the very time that state actors may be employing offensive cyber attacks, malicious ads can be deployed via apps and websites used by defense personnel, political leaders, and people maintaining critical infrastructure alike, creating national security risks for those very same states. The same structural deficits that endanger civil society, journalists, and opposition figures are potentially exploited by both foreign adversaries and cybercriminals, creating systemic risks for everyone. **These security risks make it apparent that there is an urgent public-interest need to reform digital advertising.**

The same risks apply to the private sector and to civil society. Indeed, as prior research has made clear, a large number of governments will use these potent capabilities to undermine political opposition, stealthily target journalists and lawyers, and target refugees, immigrants, and other vulnerable populations. The mercenary spyware industry is already notorious for widespread harms; fueling that industry with digital advertising capabilities will multiply those harms immeasurably.

11. Recommendations: How to Stop AdFection Attacks

The AdFection attacks and espionage described in this report impact millions of people in dozens of countries. Existing laws and self-regulation by the industry failed to catch or prevent them. In this section, we provide guidance to regulators, defenders, and the advertising industry on how to stop AdFection and ADINT-style espionage.

Advertising Vendors: Time to Get Serious

The advertising industry uses terms like “certified” and “approved” to try and convey a veneer of effective self regulation. However, the industry appears to perform no meaningful due diligence on participating vendors, instead improperly relying on self-attestation where vendors check a box on an online form. This process allows widespread privacy abuses, including failing to prevent mass espionage via targeted ads.

Ad vendors must significantly level up their cybersecurity and threat detection capacity to effectively cut off malicious advertisers across the supply chain. They must rigorously and regularly vet, screen, and audit their business partners and hold them accountable for their own supply chains. This type of more robust due diligence applies in particular to key industry organizations and dominant players who must introduce rigorous and regular audits for companies listed in ad vendor registries which they maintain and provide to many other actors in the supply chain. Business partners from countries with opaque corporate registries or where known malicious actors operate deserve specific attention.

Technical and organizational measures to be taken must include both vendor-specific and industry-wide efforts. Cybersecurity agencies and other regulators in the U.S., Canada, Europe, and other regions must support these efforts by investigating risks, calling out shortcomings and taking action to ensure the implementation of effective measures by the advertising industry.

- **Detect and block malicious ads**: Ad vendors must radically increase their capacity to identify AdFection-style attacks in real-time, alongside other forms of malicious advertising such as ad fraud, across their supply chain.
- **Share threat data**: Develop better threat sharing and clearinghouses for sharing information about malicious actors and recklessly permissive jurisdictions.
- **Vet and screen partners**: Implement mandatory know-your-customer, including due diligence and recurring vetting for all partners and other firms who transact over the provided ad and data services.
- **Audit vendor registries**: Major advertising organizations must introduce mandatory third-party audits for “certified” or “approved” vendors.
- **Ban vendors in problem jurisdictions**: Adopt a default-deny policy for vendors operating in jurisdictions known to be highly permissive of abuse, or without accountability mechanisms.
- **Fix systemic vulnerabilities**: Implement industry-wide measures to improve ad delivery security and to introduce full supply chain transparency, and support their adoption.

Zero-Click AdFection

We urge regulators to take immediate action to ensure that advertising platforms and partners stop facilitating AdFection-style attacks, and secure their populations from the security, cybersecurity, and privacy threats posed by the advertising ecosystem.

Investigation and Enforcement

- **Immediately investigate Discover-Tech and Candiru**: Our research showed large-scale data collection from millions of devices involving Discover-Tech and Candiru. The data was apparently collected for the purposes of AdFection. We urge competent authorities in all jurisdictions to investigate whether the rights of their citizens, as well as applicable privacy and security laws were violated.
- **Enforce existing laws**: It is unlikely that Discover-Tech is the only enabler of AdFection-style zero-click attacks. Authorities should more closely scrutinize the advertising ecosystem to determine whether other companies are leveraging it for espionage and spyware delivery, and determine whether they have violated applicable laws and regulations.
- **Enforcement and sanctions**: Use all necessary domestic enforcement and sanctions authorities to discourage AdFection abuse. These measures can include the use of sanctions and entity-listing powers against firms that deploy mercenary spyware and conduct espionage via targeted ads, the companies that enable them, and the individuals who work in the AdFection domain.

Legal and Regulatory Improvements

- **Commission investigations**: Enlist the assistance of cybersecurity agencies and regulatory bodies to evaluate the security, privacy, and national security risks from the current advertising ecosystem.
- **Tighten privacy regulations around ad tracking and targeting data**: Evaluate legislation to remove personal data from RTB auctions and work with international partners to adopt similar measures.
- **Real regulation of the advertising industry**: It is time for regulators and lawmakers to develop frameworks based on mandatory oversight with clear enforcement mechanisms and penalties for violation.
- **Independent audits and KYC**: Require that the advertising industry implement third-party audits and know-your-customer standards for all their business partners, as well as companies included in “certified” vendor registries. Develop meaningful penalties for failure to comply or misrepresentation.

Securing National Infrastructure Requires Blocking Ads and Tracking on Official Devices

- **Mandatory ad-blocking on government devices**: Issue policy guidance aligned with relevant cybersecurity agencies (e.g., CISA and NSA in the U.S.) recommendations requiring ad-blocking software on edge devices, and ad-blocking at the gateway for all government-owned devices. (See, for example, U.S. Senator Ron Wyden’s letter to the CIO of the U.S. Department of Defense, as well as Senator Wyden and Rep. Harrigon’s joint letter to the Inspector General of the U.S. Department of Defense).

- **Opt-out of ad targeting**: Mandate the disabling of unique advertising IDs on all government mobile devices (such as through MDM), and issue guidance and policy recommendations for personal devices used in governmental spaces.
- **Ban browsers that facilitate data harvesting**: Evaluate the security risks of browsers with impossible-to-disable tracking, and consider provisionally banning them from governmental networks and devices.

Defenders: Ad-Blocking Is A Cybersecurity Best Practice

AdFection attacks demonstrate that online advertising is now a vector for zero-click spyware infection into your organization. Taken together with research showing that data from targeted advertising is already being used for mass espionage, and potentially for corporate espionage, this makes it clear **there is currently no consistently safe way to expose your users and networks to targeted ads**. You can directly block Discover-Tech's current methods by blocking advertising identifiers, however we suspect that the AdFection attack surface may be larger, requiring more systematic measures.

- **Block ads and tracking on devices and at the gateway**: Where possible, block online advertising at the gateway to your organization, and on work-issued and edge devices. Opting out of ad targeting (such as through MDM) on company-issued devices is also advisable. We also encourage you to develop guidance and easily actionable tools to help your personnel protect their devices.
- **Transition towards browsers with less tracking**: Browsers with built-in anti-tracking features, ad-blocking, and support for the Global Privacy Control (GPC) will improve your security posture and protect your IP.
- **Scrutinize targeted ads**: We encourage defenders to monitor traffic linked to advertising impressions for signs of malicious requests.

Protecting Yourself from AdFection

AdFection is a complex threat, and if you face elevated risk because of who you are or what you do, we strongly recommend seeking expert help. However, there are certain actions you can take to reduce some AdFection risks.

- Increase your overall security by following personalized instructions from the Security Planner.
- Use a trusted ad-blocking extension on your browser to reduce tracking.
- Consider using a privacy-respecting browser that blocks tracking and data-harvesting.
- Regularly reset your Mobile Advertising ID, disable ad-tracking, and use opt-out features of apps.
- Consider using an ad-blocking service on your network, such as at your home router, or use a trusted commercial VPN service that offers ad-blocking.

Further Research

Our investigation found that an attacker that we call **DARK CARTOGRAPHER** used Discover-Tech ads and a number of additional vendors to deanonymize users at scale since at least 2019. As these efforts rely on the exploitation of widespread security issues across numerous mobile providers, disclosure to providers is in progress. We will release a subsequent report delving into technical analysis and attribution of these attacks once the disclosure process is complete.

Based on our findings, we believe that further research would be fruitful with respect to:

- customers and victims of the ad-based spyware deployment capabilities provided by Discover-Tech and the companies linked to it, including Candiru, Bindecy, and Intelos;
- additional vendors and vendor networks that deploy ad-based spyware; and,
- technical, organizational, regulatory, and political measures that effectively prevent the distribution of spyware via digital advertising.

This report is part of an ongoing series of investigations we are doing on surveillance technologies that rely on digital advertising. We will be publishing subsequent investigations that explore areas for further research we have flagged in this report.

Correspondence with Companies

We sent requests for comment to Discover-Tech Ltd, Candiru (Integrity Labs), Bindecy, Intelos, Adtimizer Ltd., Volasim Ltd., Beeswax (FreeWheel), Eskimi, Xandr (Microsoft Advertising), Vungle (Liftoff), Sunteng, IAB Europe, and Affle. We gave each company a chance to respond before a specific deadline, and committed to publishing any response received before that deadline.

Discover-Tech Ltd, Candiru (Integrity Labs), Bindecy, Intelos, Xandr (Microsoft Advertising), Sunteng, IAB Europe, and Affle did not respond to our request for comment within the timeline provided.

On October 11, 2026, we received a response from Adtimizer Ltd. In its response, Adtimizer Ltd claims that the adtimizer.[co] subdomains we consider to be linked to Discover-Tech were “used solely within Discover Tech’s infrastructure, which was entirely separate from ours and was not operated, managed, or controlled by Adtimizer”, and that Adtimizer “had no knowledge of, or involvement in the alleged activities” with respect to Discover-Tech’s malicious ad targeting. The company’s full response is available here.

On October 12, 2026 we received a response from Volasim Ltd. In its response, Volasim states that Discover-Tech was among the “external advertising providers” it engaged to “promote its products”. Volasim emphasizes in its response that it “has no involvement whatsoever in the spyware-related activities” discussed in our investigation, and that it has “never commissioned, authorized, participated in, or knowingly facilitated any such activity”. The company’s full response is available here.

On October 12, 2026, we received a response from Vungle (Liftoff), stating: “We have paused all Discover-Tech Ltd. access while we conduct our own review. Because this review is ongoing, we are not currently in a position to confirm or comment on the specific factual assertions in your letter. We will take any further action warranted.”

On October 13, 2026, we received a response from Beeswax (FreeWheel / Comcast), stating as follows: “Beeswax constantly monitors traffic quality and security threats to its Buyer Cloud platform through internal controls and third-party detection tools. Based on activity we observed recently, and after independent third-party security specialist validation, Beeswax already acted to remove Discover-Tech from Buyer Cloud. Malicious advertising of any kind is prohibited on our platform, and we will keep working with our security partners and the wider industry to detect and remove bad actors.”

On October 14, 2026, we received a response from Eskimi, stating: “Eskimi has clear rules and controls designed to detect and stop advertisers who try to misuse our platform. Campaigns and creative tags are screened by independent third-party ad-verification vendors as well as by our own monitoring tools. In this case, the advertiser’s tags were built to evade automated scanning. They loaded different code depending on who was viewing the ad, including the device, IP address and location, and campaigns were often restricted to very narrow IP target lists. This is how they passed third-party verification. Our own monitoring flagged this behaviour, and campaigns and individual tags were stopped as our controls detected them. We have since shared the relevant technical indicators with our supply partners. In the interest of supporting your research, the indicators we identified include creative tags calling remote “getAd” loaders hosted on dtech.adtimizer.co, several mtrtb.com subdomains (noas, infinoas and ppv2), and events.myweb3id.io. Because these loaders served different code depending on the viewer and targeting, they were not detected by third-party ad-verification scanning. Additional technical information can be provided where it is useful for your research. Discover-Tech had been a self-service advertiser on the Eskimi DSP since 2022, under our standard advertiser terms. Because of our campaign and individual tag blocks, its activity remained small, amounting to only a few hundred dollars in media spend. Its last campaign through the Eskimi DSP was stopped on 6 August 2026, and no impressions have been served since. Once the full pattern of the advertiser’s behaviour became clear, we permanently blocked all of its accounts, users and associated domains. We are working with independent ad-security specialists to help identify similar behaviour across the industry. As I mentioned, happy to contribute with anything that can help with further investigation and ensuring compliance in the ad-tech market.”

Google, which collaborated in the investigation, informed us that it “terminated Discover-Tech’s access to its ad exchange platforms, blocking them from bidding or serving ads across our ecosystem. Google has also deployed Safe Browsing protections to warn users that may encounter known actor-controlled domains”.

While IAB Europe did not respond to our request for comment within the timeline provided, we received a response on October 15 which we have published here.

Note on Research Ethics

All research involving human subjects conducted at the Citizen Lab is governed under research ethics protocols reviewed and approved by the University of Toronto's Research Ethics Board.

Acknowledgements

We thank the teams at Al Jazeera for graciously consenting to our investigating this case, and agreeing to be named in the report.

We thank the teams at Confiant, Google, and additional researchers for their assistance and collaboration in this investigation. We would also like to thank Rebekah Brown, Maia Scott, and Krzysztof Franaszek (Adalytics Research) for peer reviewing this work, as well as other anonymous peer reviewers. Thanks to Adam Senft, Aly Bruce, Anna Mackay, and Claire Posno for editorial and communications support.

Appendix A. Ad Vendors Involved in Discover-Tech's Ad Operations

Google and Yandex

Google dominates the digital advertising ecosystem in the U.S., Europe, and other regions. It operates a massive ad exchange and systems for ad sellers (Ad Manager, AdSense, AdMob) and ad buyers (Google Ads, DV360). Its "Authorized Buyers" program allows third-party ad vendors to deliver ads by participating in ad auctions on Google's ad exchange.

Yandex, although much smaller in revenue, similarly dominates the digital advertising ecosystem in Russia and some other regions. It also provides both an ad exchange and systems for ad sellers and buyers.

Beeswax, Owned by Freewheel/Comcast

Beeswax is a major US-based ad buying platform, since 2021 owned by Comcast's ad platform FreeWheel. It offers a Demand-Side Platform (DSP) that helps advertisers and other ad vendors deliver targeted ads to users by participating in ad auctions. Its "bidder-as-a-service" product is considered highly customizable and imposes fewer restrictions on its clients than other DSPs.
The FreeWheel website states that, by using Beeswax' ad buying platform rather than other DSPs, clients could "access the full, unfiltered stream of RTB events, in much the same way [they] would if [they] were building a bidder from scratch". Clients can augment the stream of ad bidding data they receive, for example, by "mapping" users to "rich profiles", and they can use custom bidding algorithms and targeting attributes.

While this appears to offer great flexibility to clients to an extent that may come close to operating their own DSP, FreeWheel takes care of the integrations with ad exchanges and Supply-Side Platforms (SSPs) that help app and website publishers sell ads. As of July 2026, the FreeWheel website lists integrations with 36 "supply partners" including Google, Amazon, Microsoft, Index Exchange, and many others.

Beeswax is listed as an approved TCF ad vendor by IAB Europe (vendor list). Google lists Beeswax as a certified ad vendor and among its "common" European ad technology partners which Google will use by default when publishers do not set up a custom list of ad vendors. For its ad serving and third-party tracking, Beeswax uses the domain bidr[.]io and the cookie identifier bito (devicedisclosure.json).

Eskimi, a White-Label DSP Based in Lithuania

Eskimi is a digital advertising group based in Lithuania with offices in Greece, Turkey, Japan, United Arab Emirates, Indonesia, Bangladesh, Nigeria, and Kenya, according to its website, eskimi.com. Its ad buying platform Eskimi DSP, which allows its clients to target 1.5 billion "profiled users" across 60 ad exchanges, according to the company, is also offered as a "white-label" version that "enables agencies, ad networks, and businesses to offer 'Eskimi DSP' under their own brand". Eskimi also provides a data management platform (DMP) that "collects and stores data" it receives from 50 ad exchanges, amounting to two2 billion profiles, according to a 2025 version of the company's website. Its website and Lithuanian company records show that it is incorporated as "UAB Eskimi", also known as "UAB Aktyvus sektorius."

Eskimi is much lesser known than Beeswax. Except for two paid posts, we did not find any articles discussing the company on digital advertising trade press sites like Adweek, Digiday, and AdExchanger. Eskimi was, however, prominently discussed when US-based data broker Datastream Group told U.S. Senator Ron Wyden that Eskimi was the source of 3.6 billion location data records revealing the exact movements of millions of people, including U.S. military and intelligence personnel, as reported in a joint investigation by German netzpolitik.org and other outlets. This investigation has helped spark extensive debates about ad surveillance.

While German netzpolitik.org found several additional links between the analyzed data and the company, Eskimi denied that it was the source of the data. Google told 404 Media that Eskimi is "part of Google's Authorized Buyer program and must abide by our policies". It added that it "regularly audits its Authorized Buyers program participants". Eskimi is closely linked to the location data broker Redmob, which claims to sell data on one billion people across 150 countries according to its website, redmob.io. While Redmob is incorporated in Dubai, netzpolitik.org found that Eskimi and Redmob share the same CEO, who responded to their questions about Eskimi from a Redmob email address.
As of July 2026, Eskimi is listed as an approved TCF ad vendor by IAB Europe (vendor list). Google lists Eskimi as a certified ad vendor and among its European ad technology partners.

Vungle, Liftoff's SSP, and Ad Exchange

Vungle was a mobile advertising firm that merged with the U.S.-based mobile advertising firm Liftoff, which went public in June 2026. Since the merger, Liftoff offers several Vungle-branded products including a Supply-Side Platform (SSP) named Monetize, which helps app publishers sell ads, and the mobile ad exchange Vungle Exchange, which helps marketers buy ads served in mobile apps.
Both the SSP and the ad exchange rely on the Vungle SDK, which is a piece of advertising and tracking software embedded in many Android, iOS, Amazon, Windows, and Unity apps. The Vungle SDK is embedded in 150,000 mobile apps used by one billion people across 150 countries, which also describes the number of users that can be targeted via the Vungle ad exchange, according to the company.

Guidelines for the Vungle ad exchange contain a rule that asks clients to "refrain from" using the platform for the distribution of "malware, spyware, and files that can harm or gain unauthorized access to a device or user information". We did not find an explanation of how the company monitors and enforces this rule.

Vungle has been controversially discussed in several papers and reports on mobile tracking and privacy. The Norwegian Consumer Council found in 2020 that Vungle received GPS coordinates and other personal data on users of Grindr and another mobile app, seemingly without a legal basis under the GDPR.

As of July 2026, Liftoff's "Monetize" and "Vungle Exchange" products are listed as approved TCF ad vendors by IAB Europe (vendor list). Google lists Liftoff's DSP and Monetize products as certified ad vendors and it lists Liftoff among its "common" European ad technology partners that Google will use by default when publishers do not choose a custom list of ad vendors.
Google has been deeply interconnected with Vungle from its inception. Google Ventures was an investor in Vungle's seed, series A, and series B funding rounds. The Norwegian Consumer Council pointed out in 2020 that Google's mobile advertising system AdMob "provides Vungle with access to extra features that allow Vungle to bypass data filters, and thus send more data to its partners than what would ordinarily be possible through Google's regular advertising tools". As of July 2026, Liftoff's Vungle product Monetize is listed among a few "premium bidding partners" in Google's mobile advertising system AdMob and among a few "ad sources" for AdMob's advertising services on Android and iOS.

Sunteng, a Chinese SSP, DSP, and Ad Exchange

The Chinese digital advertising firm Sunteng provides ad buying and selling services for both advertisers and publishers, as well as a "programmatic marketplace", i.e. an ad exchange, according to its website, sunteng.com. The site also refers to the company as "Shunfei Technology". The link to Sunteng's DSP offering leads site visitors to biddingx.com ("BiddingX"), an entity that promotes itself as China's largest DSP. Sunteng appears to operate also under the brand Bidex (bidex.cn), which focuses on "overseas programmatic", i.e. on digital advertising services for non-Chinese clients. We assume that Sunteng,

Shunfei, Bidex and BiddingX are part of the same Chinese group of companies with offices in Singapore and the US. Sunteng claims to process 50 billion ad bid requests a day across 10,000 mobile apps and 60 ad vendor partners, and it lists Eskimi as a partner.

As of July 2026, Google lists biddingx.com ("Shunfei Infomation Technology Corporatio" [sic]) as a certified ad vendor. IAB Europe listed bidex.cn ("Sunteng Hong Kong Holdings Limited") as an approved TCF ad vendor until December 2025 (vendor list).

Xandr, aka Microsoft Advertising

Xandr, formerly known as AppNexus, has long been a major player in digital advertising. After Microsoft acquired it from AT&T in 2022, it became part of Microsoft Advertising in 2023. While Microsoft shut down Xandr's ad buying system, the "Invest" DSP, in early 2026, it continues to offer Xandr's ad selling system, the "Monetize" SSP. Ad buyers who used the former Xandr DSP were "handed" to Amazon DSP, according to trade press reporting.

As shown in Section 6, Microsoft's user ID syncing in the browser via the domain adnxs[.]com, which assigns a Microsoft user ID to people who visit the sites of ad sellers and maps it to user IDs assigned by other ad vendors, appears to remain operational as of June 2026. Xandr has long been operating massive identity databases. In 2020, when Xandr was still owned by AT&T, it reportedly operated an identity graph linking 5 billion identifiers.

As of July 2026, Microsoft's ad system Xandr is listed as an approved TCF ad vendor by IAB Europe (vendor list). Google's list of certified ad vendors contains four records for Xandr. Google also lists Xandr among its "common" European ad technology partners which Google will use by default when publishers do not choose a custom list of ad vendors.

Appendix B. Glossary

Adtech vendor, ad vendor. Advertising technology intermediary such as a Demand-Side Platform (DSP), Supply-Side Platform (SSP) (both defined below) or ad exchange.

Ad Slot. Designated space or position on a website or mobile app reserved to display an ad.
Demand-Side Platform (DSP). System operated by an adtech intermediary that helps advertisers buy ad placements across many different websites or mobile apps in an automated way by participating in real-time auctions hosted by ad exchanges.

Supply-Side Platform (SSP). System operated by an adtech intermediary that helps publishers of websites or mobile apps sell ad slots in an automated way by participating in real-time auctions hosted by an ad exchange, which is often operated by the same ad vendor as the SSP.

Ad Exchange. Automated marketplace operated by an adtech intermediary that hosts real-time auctions which facilitate the selling of ad slots and the buying of ad placements across many publishers, advertisers and intermediaries like DSPs and SSPs. Ad exchanges are often operated by SSPs.

Real-Time Bidding (RTB). Automated high-frequency auctions hosted by ad exchanges where advertisers (or DSPs on their behalf) bid on ad placements offered by website and mobile app publishers (or their SSPs). When a user visits a website or uses an app that sells targeted ads via RTB, the publisher's SSP initiates a bid request that transmits data about the user and the ad slot to several DSPs, who submit bids on behalf of advertisers. The ad exchange determines the winner of the auction and pushes the ad to the user.

Bid Request. RTB auction record that describes an ad slot and the user who currently visits a website or uses a mobile app. Bid requests are initiated by publishers and sent via an SSP and an ad exchange to several DSPs, which place bids in order to show ads to specific users on behalf of advertisers. Bid requests typically contain personal data about users in order to facilitate targeted advertising.

Mobile Advertising ID (MAID). Unique identifier for a mobile device used for advertising and tracking purposes, assigned by the device's operating system such as Google Android or Apple iOS. While users can reset or delete mobile ad IDs in the settings, they are activated by default. Advertising and data companies use mobile ad IDs to link user data across contexts and vendors in order to track, follow, profile and target users.

Cookie ID. Unique identifier for a user's web browser, typically stored and retrieved in the browser by third-party code operated by adtech vendors during website visits.

Appendix C. Domains Linked to Discover-Tech and Controlium

General

We assess that the following domains are – or have been – linked to Discover-Tech and Controlium:

```
*.discover-tech[.]io
*.mtrtb[.]com
*.mydsp[.]io
*.controlium[.]net
*.powerium[.]net
*.platc-tester[.]com
*.myweb3id[.]io
*.myipinfo[.]io
*.akedo[.]gg
*.volasim[.]com
```

NOAS Servers

According to our analysis, Discover-Tech operates – or has operated – the following NOAS servers as part of its Controlium platform:

```
noas.mtrtb[.]com/getAd
infinoas.mtrtb[.]com/getAd
ppv2.mtrtb[.]com/getAd
pqv2.mtrtb[.]com/getAd
events.platc-tester[.]com/cplatform/getAd
events.myweb3id[.]io/cplatform/getAd
noas.powerium[.]net/getAd
qa-noas.powerium[.]net/getAd
```

Additional NOAS domains that appear to be associated with Discover-Tech:

```
noas.adtimizer[.]co
noas.impchkdsp[.]com
noas.trakking[.]co
```

Ad Tracking Domains

We assess that the following additional domains are – or have been – associated with Discover-Tech's ad tracking or targeting:

```
tracookiepixel[.]xyz
cookiesurfer[.]com
cookie-sync[.]xyz
ads-monitor[.]xyz
checkmyimp[.]com
ads-impressions[.]com
nutralove[.]co
```