CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

December 3, 2025


# Intellexa's Global Corporate Web

**Insikt Group found more companies likely tied to Intellexa's wider network,** especially to the previously reported Czech cluster, including one seemingly used to ship Intellexa products to clients.

**Two newly identified advertising firms may link to the "Aladdin" ad-based infection vector,** previously tied to the Czech cluster via a leaked 2022 proof-of-concept invoice.

**Insikt Group continues to observe Intellexa activity across multiple countries,** including Iraq, even as the group has changed its infrastructure setup and techniques.

*The author, Julian-Ferdinand Vögele, thanks Amnesty International's Security Lab for its ongoing reporting on the Intellexa and Predator spyware ecosystem. Today, Security Lab published a related report on Intellexa, which can be found here.*

NOTE: This was updated on February 20, 2026, with a minor correction.

## Executive Summary

Insikt Group identified several individuals and entities linked to Intellexa and its broader network of associated companies. These connections span technical, operational, and corporate roles, including backend development, infrastructure setup, and company formation. Using export and import data, Insikt Group identified one entity linked to the previously reported Czech cluster that facilitated the shipment of Intellexa products to clients. In at least one instance, a direct delivery was made to an end user, while additional entities in Kazakhstan and the Philippines appear to have been involved in product imports, indicating an expanding network footprint. Two additional entities in the advertising sector may be tied to the "Aladdin" ad-based infection vector, previously associated with the Czech cluster via a leaked 2022 invoice. In addition, Recorded Future's proprietary intelligence revealed ongoing Predator spyware activity in multiple countries, including new evidence of its deployment in Iraq.

The continued domestic use of mercenary spyware such as Predator poses significant privacy, legal, and physical security risks worldwide. Although civil society remains the primary target in most publicly documented cases, recent evidence shows that executives and other high-profile individuals with substantial intelligence value are increasingly being targeted as well. Due to Predator's costly licensing model, operators are likely to reserve its deployment for high-value strategic targets, placing politicians, business leaders, and individuals in sensitive roles at heightened risk. Meanwhile, the widespread and likely unlawful use of spyware against political opposition continues to be a pressing issue under investigation in several European Union (EU) member states, including Poland and Greece.

Insikt Group assesses that several key trends are shaping the spyware ecosystem, including growing balkanization as companies split along geopolitical lines, with some sanctioned entities seeking renewed legitimacy through acquisitions while others shift toward regions with weaker oversight (1, 2). Despite this, a core network of facilitators continues to underpin the industry's operations. Furthermore, rising competition and secrecy surrounding high-value exploit technologies are heightening risks of corruption, insider leaks, and attacks on spyware vendors themselves. Targeting has also expanded beyond traditional civil society figures to include corporate leaders and private-sector individuals (1, 2), suggesting that the publicly visible cases represent only a fraction of a much larger, concealed global ecosystem.

## Key Findings

- Insikt Group uncovered additional companies highly likely tied to Intellexa's broader corporate web, particularly within the previously discussed Czech cluster. At least one of these entities appears to have been used to ship Intellexa products to clients, offering further insight into Intellexa's global business structures.
- Two newly identified companies appear to operate in the advertising sector and may be connected to a previously reported ad-based infection vector known as "Aladdin." This vector was earlier associated with the Czech cluster through a leaked invoice from 2022 showing payments for a proof-of-concept to an individual linked to that cluster.
- Analysis of export and import databases revealed indications that one of the newly identified companies was used to deliver Intellexa products to end customers, either directly or through intermediaries. This research also exposed two additional entities located in Kazakhstan and the Philippines.

# Table of Contents

## Background

Predator is a sophisticated mercenary spyware targeting both Android and iPhone devices and has been active since at least 2019. Initially created by Cytrox and now seemingly managed and distributed through a broader network of Intellexa-linked companies, Predator is designed for adaptability and stealth, leaving little evidence on compromised devices and complicating external investigations into its misuse. Once deployed, Predator provides complete access to a device's microphone, camera, and all data, including contacts, messages, photos, videos, and more. Its modular, Python-based architecture lets operators add capabilities remotely without re-exploiting the device.

Predator can be delivered through "1-click" and "zero-click" attack vectors. "1-click" attacks rely on social engineering messages with malicious links that require user interaction (1, 2, 3), while "zero-click" attacks, described in the "Predator Files," involve techniques that do not require any action from the target, such as network injection or proximity-based methods. However, there have been no confirmed cases of Predator using fully remote "zero-click" exploits like those seen with NSO Group Pegasus, which can compromise devices through messaging apps without any user interaction (for example, FORCEDENTRY or BLASTPASS).

Over the past two years, Insikt Group has identified suspected Predator operators in more than a dozen countries, including in Angola, Armenia, Botswana, the Democratic Republic of the Congo, Egypt, Indonesia, Kazakhstan, Mongolia, Mozambique, Oman, the Philippines, Saudi Arabia, and Trinidad and Tobago (1, 2). Further investigations have revealed evidence of Predator deployments and operator activity in a number of other countries, among them Greece, Sudan, and Vietnam (see **Figure 1**). Notably, in Greece, the use of Predator against journalists, politicians, businesspeople, and other public figures, known as the "Predatorgate" scandal, has prompted multiple investigations and legal proceedings that remain ongoing.

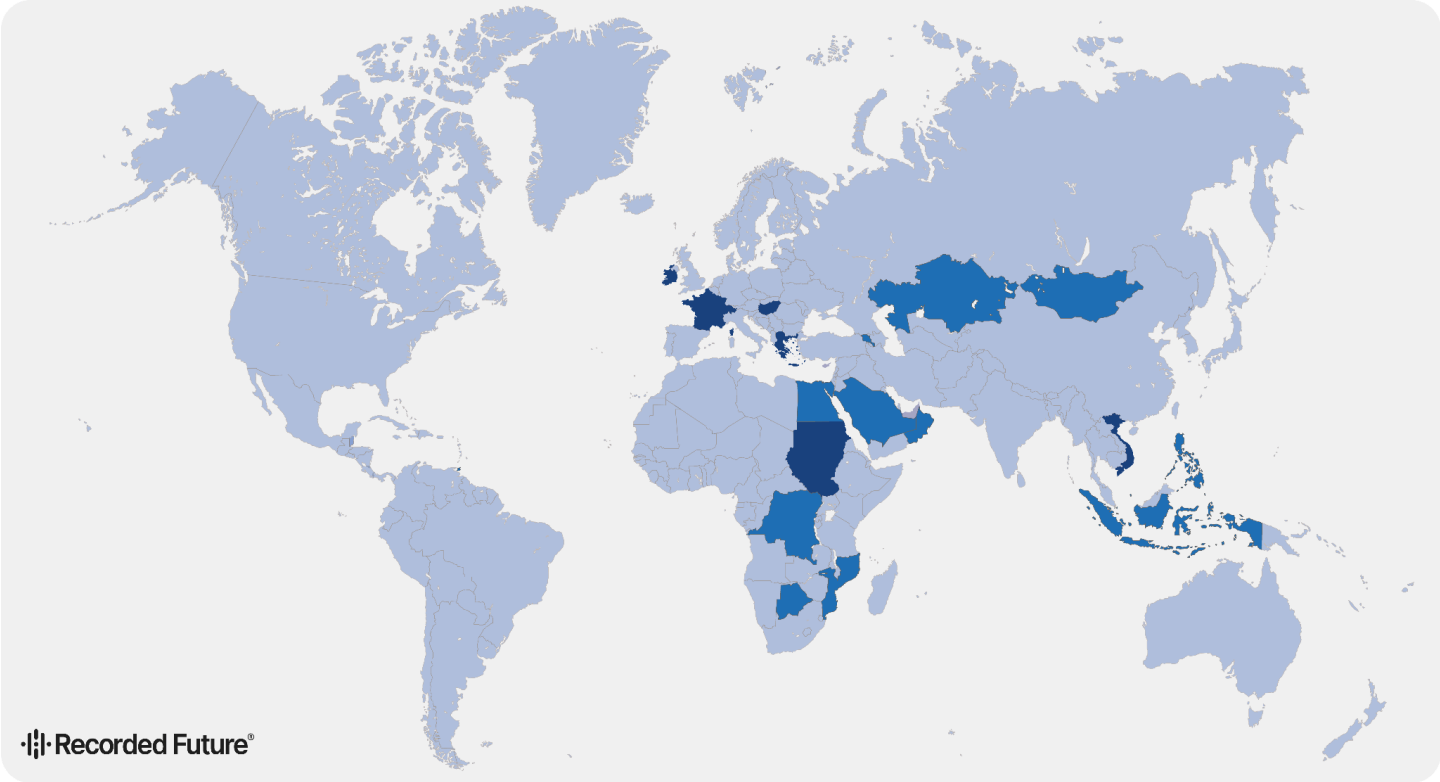


***Figure 1:*** *Countries where there is evidence of Predator deployments and operator activity (Source: Recorded Future)*

Although Predator is officially marketed for counterterrorism and law enforcement use, investigations have revealed a consistent pattern of its deployment against civil society figures, including journalists, activists, and politicians (1, 2, 3, 4). The cases documented in earlier reports likely represent only a fraction of the total abuses, given the broad proliferation of mercenary spyware such as Predator, the increasing difficulty of detection, likely exacerbated by recent iPhone operating system updates, and the limited support and awareness among victims. It is important to highlight the risk of cross-border targeting, exemplified by cases involving Predator, where an operator linked to Vietnam reportedly targeted EU officials and members of the European Parliament, as well as other mercenary spyware such as Pegasus. Lastly, although individual spyware vendors may implement different control mechanisms, statements by the CEO of Memento Labs have raised doubts about their effectiveness, as one of the company's clients reportedly continued using products that were meant to have been decommissioned.

Despite increased public reporting on Predator's infrastructure and techniques, and growing attention of Intellexa's corporate structure, Predator operations continue, though the full scope of their activity remains unclear. This persistence continues even after measures such as US sanctions, an EU resolution, a US visa ban on Intellexa affiliates, and the launch of the Pall Mall Process[1], alongside likely rising exploit costs, particularly for iPhones. This likely reflects rising demand for spyware, especially in

[1] The Pall Mall Process is an initiative launched by the governments of France and the United Kingdom aimed at establishing standards for the ethical use of commercially available technologies in intrusive surveillance operations.

countries facing export restrictions, ongoing technical innovation, and increasingly complex corporate structures (for example, front companies and unwitting directors) designed to impede sanctions and attribution.

Notably, while actual payments and terms are opaque, exploit-chain prices for smartphones like iPhones often reach the millions; for example, reports cite a Russian zero-day broker offering up to $20 million for zero-day remote code executions (RCEs) against the latest iPhones and Android devices, and a United Arab Emirates (UAE)-based startup, Advanced Security Solutions, reportedly offering up to $20 million for SMS-delivered smartphone hacking tools.

Ultimately, it remains unclear whether companies like Intellexa develop their own exploits or obtain them from others (and, if so, at what cost and under what conditions) as well as who else collaborates with these providers. A 2024 report indicating that the Russia-backed group APT29 (tracked as BlueBravo by Insikt Group) may have used the same exploits as Intellexa and NSO underscores why this issue warrants attention and raises a number of important questions.

## Mapping Intellexa's Corporate Web and State of Activity

Mapping the corporate structure of a mercenary spyware vendor such as Intellexa presents significant challenges. As illustrated in **Figure 2**, these entities typically operate through a complex web of shell and front companies distributed across multiple jurisdictions. They frequently alter ownership structures, employ ambiguity, and use various obfuscation tactics to evade detection. Consequently, the available picture of Intellexa's organizational landscape is often incomplete, opaque, and rapidly outdated.

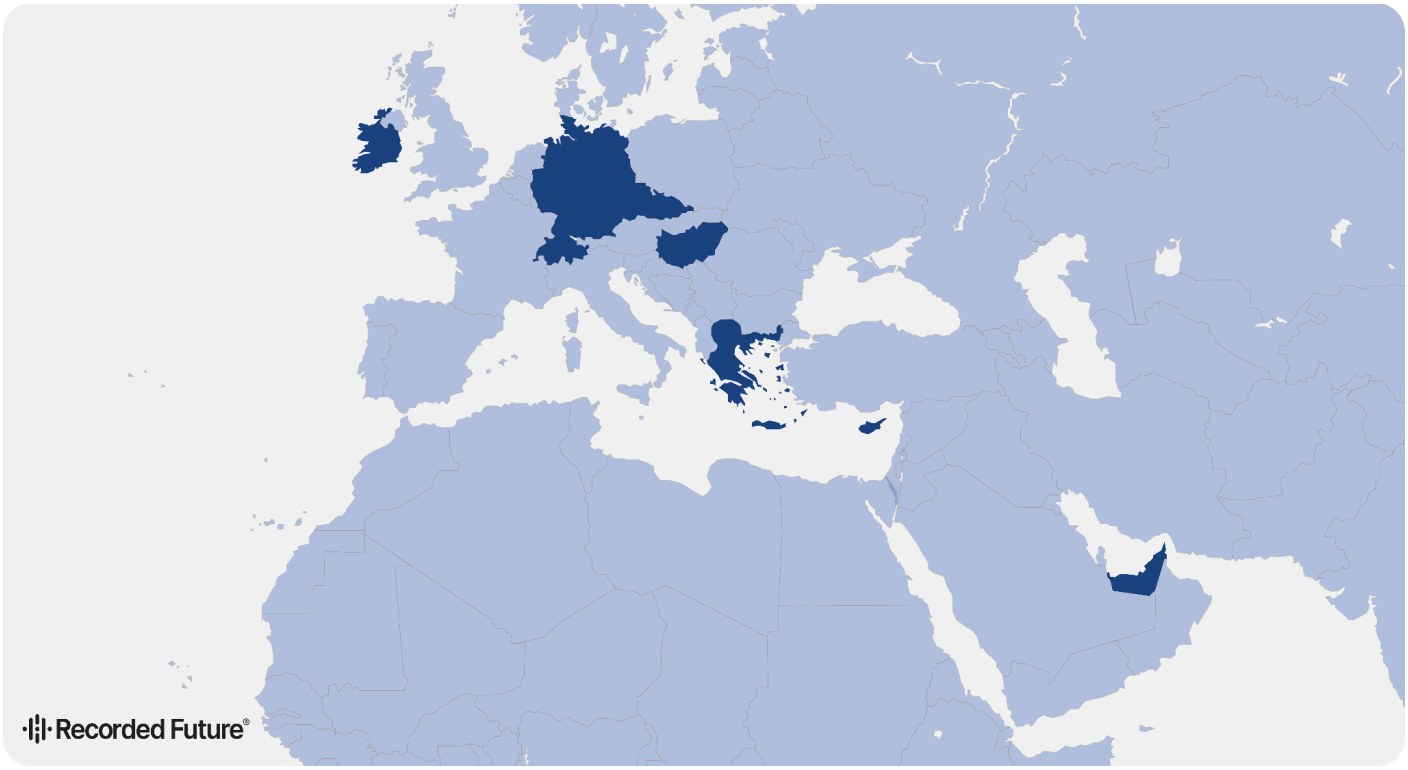


***Figure 2**: Locations of companies linked to Intellexa (Source: Recorded Future; Amnesty International)*

This report seeks to narrow some of the existing knowledge gaps by offering new insights into the structure and operations of Intellexa's corporate web. It highlights suspected Intellexa-affiliated employees, identifies additional companies that may have served, or continue to serve, as front entities, including two possibly linked to AdInt-related attack vectors, and provides further details on how Intellexa–associated firms appear to ship their products to end customers.

## Intellexa Employees and Risks of Corporate Fragmentation

Using proprietary Recorded Future data, Insikt Group gained deeper insights into several partially identified employees. Among them, three are likely based in Greece and one in North Macedonia. Available information suggests these individuals are, at least in part, involved in infrastructure, development, legal, and IT support–related activities.

- The first individual, based in Greece, has a professional background in IT administration across logistics and consulting sectors, uses multiple Intellexa-linked and related company email addresses, and shows evidence of IT infrastructure involvement through various technical platforms.
- The second individual is assessed to be part of Intellexa's infrastructure team, with activity through Intellexa-linked accounts accessing IT management services from the same system as the first individual.
- The third individual's email appears in company records for several Intellexa-linked entities, all represented by a Greek lawyer involved in multiple international legal and business contexts.

- The fourth individual, based in Skopje, is a backend developer with past roles at regional telecom firms, a "stealth mode" company tied to Cytrox, and later at another European cybersecurity firm, with additional online activity linked to development platforms and repositories.

### *Role of Greece in Intellexa-Linked Operations*

Notably, the 2023 Predator Files previously reported that Athens had become a central hub for Intellexa operations. According to the investigation, a former employee of Cytrox, a subsidiary of Intellexa responsible for developing Predator, stated that a training center for Predator operators had been established in Athens. This facility, originally planned for Skopje, was reportedly overseen by an individual referred to as "Greek Cypriot." Based on a leaked 2021 commercial proposal, comprehensive training and round-the-clock remote operational and technical support had been previously discussed.

A report published in November 2025 revealed that Intellexa had allegedly conducted covert training sessions within the offices of the Greek security contractor Krikel. The company appears to have played a role in procuring or facilitating the use of Predator spyware in Greece, an involvement that ultimately contributed to what became known as "Predatorgate." The Greek offices of both Intellexa and Krikel were raided by the Greek police cybercrime division as part of the ongoing investigations into the wiretapping scandal. Legal proceedings related to "Predatorgate" remain ongoing at the time of writing.

According to an Inside Story report from April 2024, several former Intellexa employees were allegedly connected to IANUS Consulting, Remote Greece, and ADDAPP Technologies, which were said to serve as intermediaries for employee compensation. While the precise nature of these companies' relationship with Intellexa remains unclear, Inside Story reported that ADDAPP Technologies' response to a request for comment originated from the same tax domicile and business address services provider used by Intellexa-affiliated entities, including Apollo Technologies and Hermes Technologies.

### *Risks of Corporate Fragmentation in Mercenary Spyware Ecosystem*

Corporate fragmentation within the mercenary spyware ecosystem, and the surveillance industry more broadly, does not merely complicate structural analysis; it also introduces distinct operational and security risks that can ultimately affect end customers. These risks can be grouped into three primary categories:

- **Increased security vulnerability:** As corporate structures become more fragmented and less streamlined, network hardening becomes significantly more challenging. In cases such as Intellexa, this complexity likely increases susceptibility to cyber attacks and security lapses. This is particularly concerning given that mercenary spyware vendors appear, at least in part, to retain visibility into their customers' operations, a risk previously exemplified by the NSO Group.
- **Operational constraints due to sanctions and covert operations:** Sanctions and the need for covert or semi-clandestine operations make it more difficult for these entities to obtain certain technologies or technical support. This limitation may compel them to rely on personal devices, third-party providers, or informal channels, thereby increasing exposure to security risks.

- **Employee-related exposure risks:** As illustrated by the individuals discussed earlier, employees linked to companies like Intellexa may, through secondary engagements or contracting roles, gain access to external networks, including potentially sensitive or intelligence-sharing environments. Such overlap could inadvertently create pathways for data exposure or unauthorized access to intelligence.

## Revealing Additional Elements of the "Czech Cluster"

Through additional corporate research, Insikt Group identified a new set of companies highly likely linked to Intellexa, tracing their connections through a previously reported cluster of firms in the Czech Republic associated with Dvir Horef Hazan (see **Figure 3**).

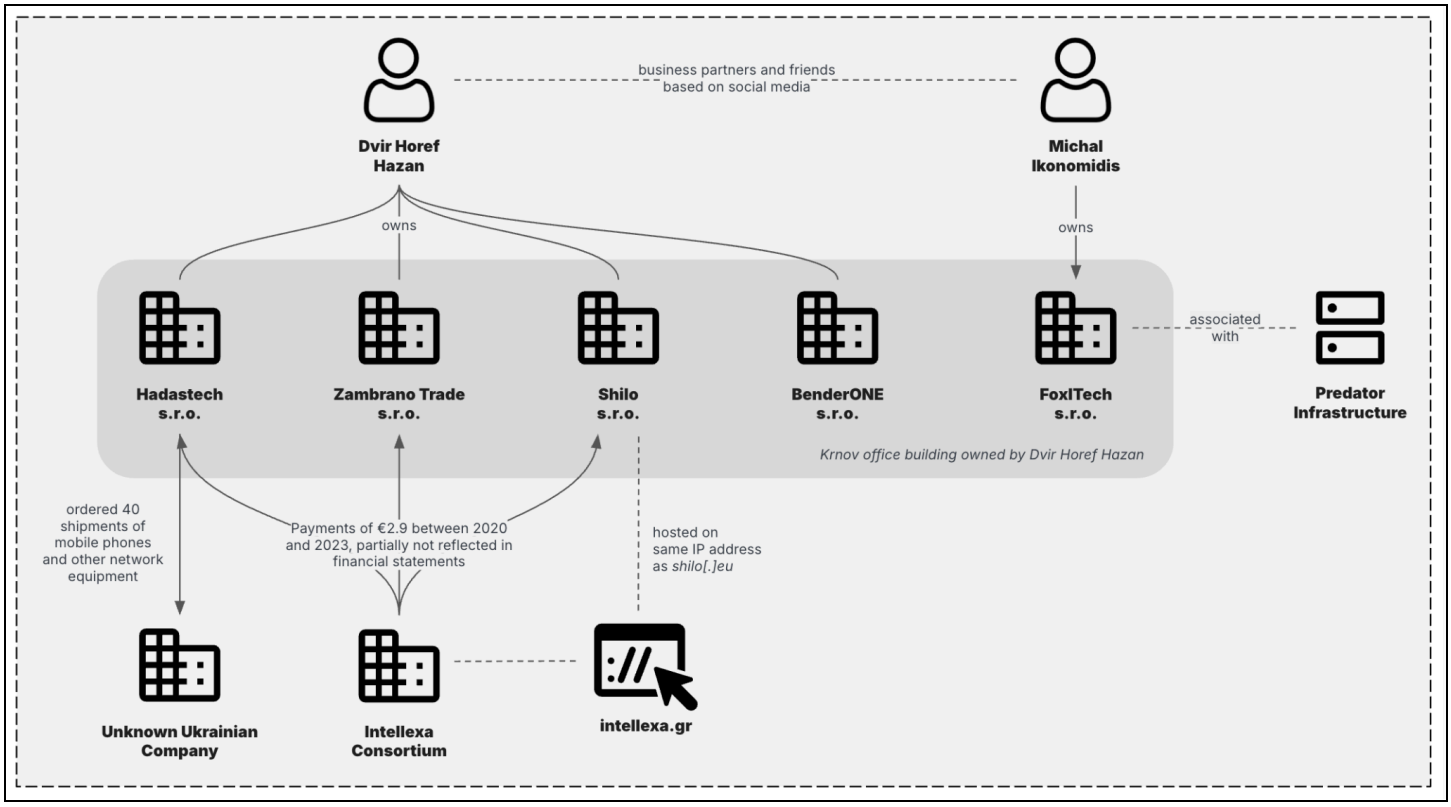


***Figure 3**: Connections between Predator infrastructure and FoxITech s.r.o. (Source: Investigace.cz; Recorded Future)*

Both the newly identified entities and the previously reported companies connected to this Czech cluster are illustrated in **Figure 4**. These companies appear to fulfill distinct operational roles within the broader Intellexa network, which are examined in the following sections. Notably, the domains associated with the four new entities discussed below became active in close succession between March 8 and 26, 2024.

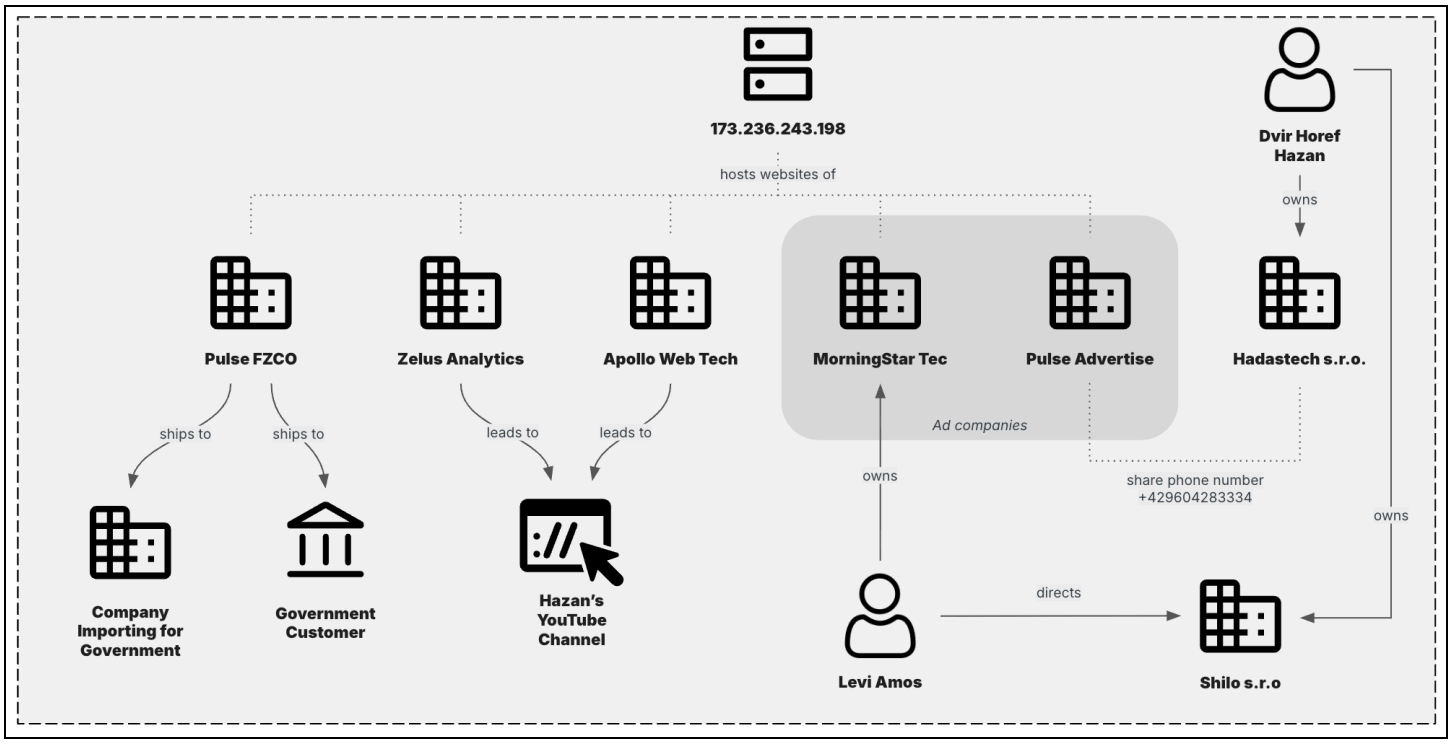


***Figure 4**: Further mapping of Intellexa's corporate web linked to Czech cluster (Source: Recorded Future)*

### *PULSE FZCO — Cyber Security Consultancy*

The company PULSE FZCO is associated with the domain *pulse-fzco[.]com*, which was hosted on the IP address *173[.]236[.]243[.]198* (DREAMHOST-AS, US [AS26347]) from at least March 10, 2024, until the time of writing. The IP address has also hosted other Intellexa-associated domains such as *shilo[.]eu* and *thalestris[.]ch*, as well as other domains linked to newly identified companies discussed in this report. PULSE FZCO is registered in the Dubai International Free Zone Authority (DIFZA) in the United Arab Emirates (UAE) and, according to its website, claims to "help you safeguard your data from cyber threats, data breaches, and unauthorized access" (see **Figure 5**).

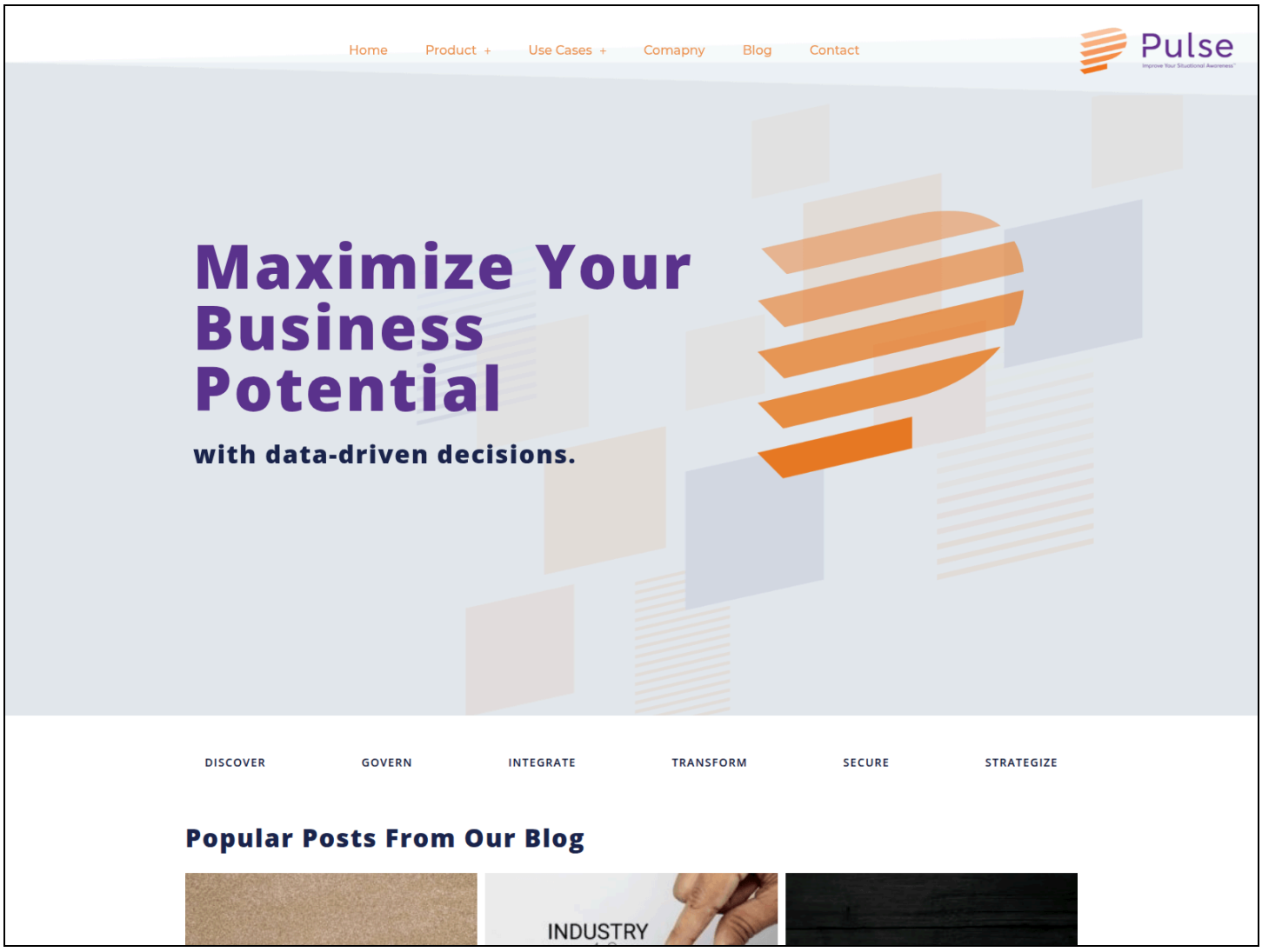


***Figure 5**: Website linked to PULSE FZCO (Source: URLScan)*

Based on export data analyzed by Insikt Group, PULSE FZCO likely operates as a front company used to facilitate product shipments, either directly to Intellexa clients or through local importing partners, as discussed further in the section titled **Tracing Previously Identified Intellexa Customers through Export Data**.

Interestingly, the Pulse FZCO website lists a company named SefuTech as one of its partners.

### *Zelus Analytics*

The company Zelus Analytics is linked to the domain *zelus-analytics[.]com*, which was hosted on the same IP address as the domain linked to PULSE FZCO. The domain was resolving to this IP address from at least March 8, 2024, two days prior to the registration of PULSE FZCO's domain, until October 28, 2025, when it ceased resolving to that IP address. According to its website, Zelus Analytics claims

to provide "a unique data analysis system designed to process large amount of data from multiple sources and diverse formats including text, voice, images, location, calendars, contacts metadata and more to provide a complete and holistic intelligence image for intelligence investigation purposes" (see **Figure 6**). The system is referred to as TCDA (Target Centric Data Analytics).

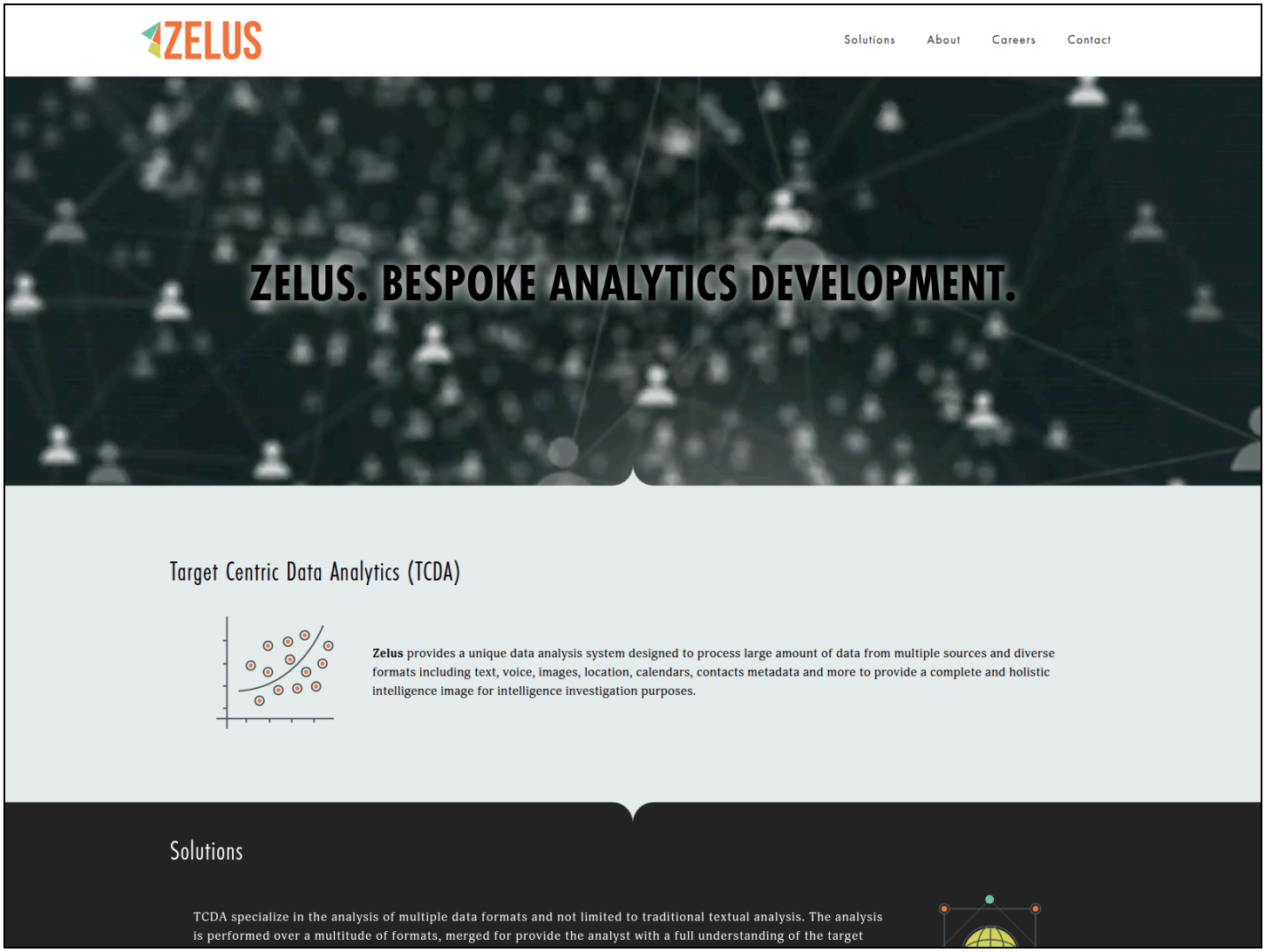


***Figure 6**: Website linked to Zelus (Source: Recorded Future)*

Notably, Zelus in Greek mythology is the daimon personifying dedication, rivalry, envy, jealousy, and zeal, a noteworthy detail given that several previous companies, including "Apollo" and "Hermes," also drew inspiration from Greek mythology.

Within the document object model (DOM) of the Zelus Analytics website, a link was found that resolves to the YouTube video uploaded by @dvir-horefhazan7938, an account highly likely belonging to Dvir Horef Hazan (see **Figure 7**). Interestingly, a link to the same video was also found on the website *apollowebtech[.]com*, which has been hosted on the IP address *173[.]236[.]243[.]198* since at least March 13, 2024.

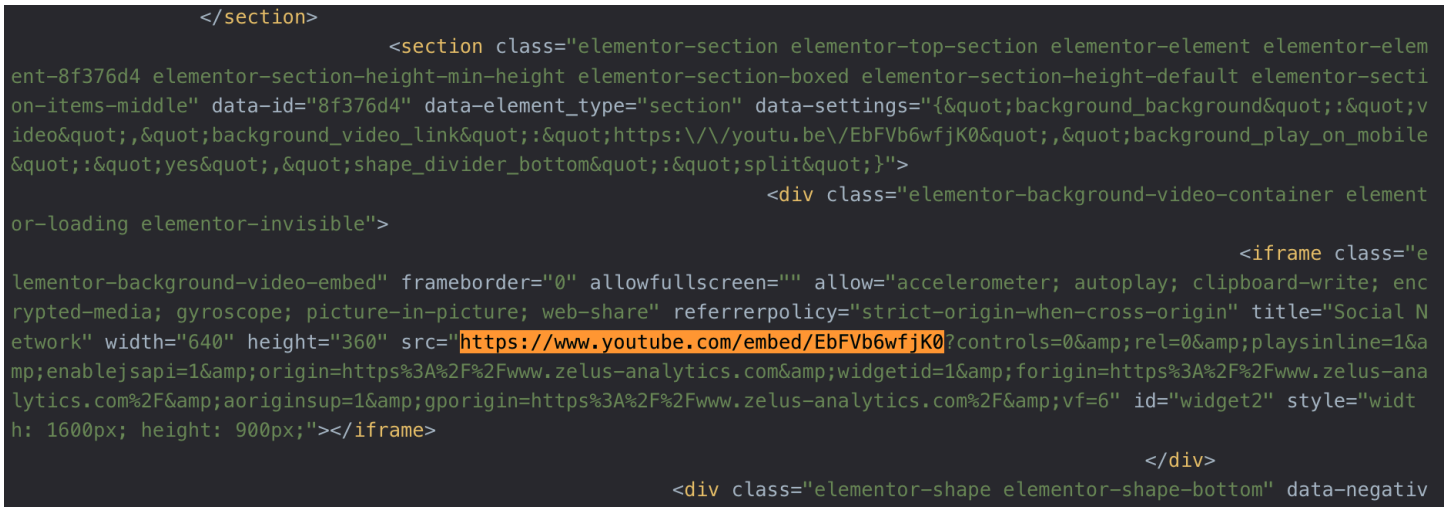


***Figure 7**: DOM on the website hosted on* apollowebtech[.]com *(Source: URLScan)*

The website on *apollowebtech[.]com*, which is likely linked to the known Intellexa-related company Apollo Technologies discussed above, claims to be a "leading provider for Law enforcement and Intelligence agencies worldwide" (see **Figure 8**).

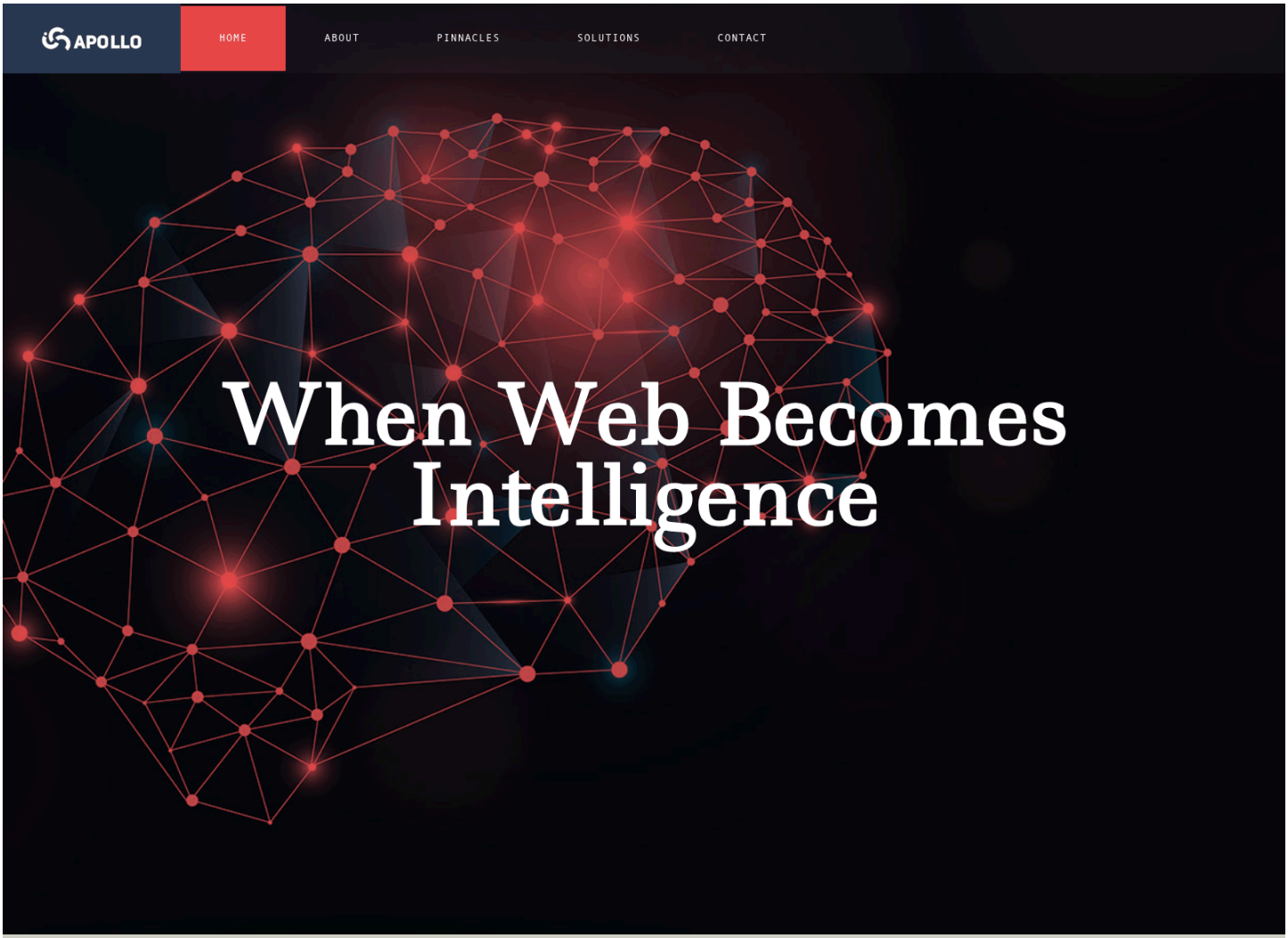


***Figure 8**: Website linked to* apollowebtech[.]com *(Source: URLScan)*

The YouTube video is brief and depicts a zoom-in sequence of a "Social Network," as illustrated in **Figure 9**. While its exact purpose remains unclear, it is assessed that the video was likely intended to lend an appearance of legitimacy to the website or served merely as a placeholder element.


***Figure 9**: YouTube video linked to Dvir Horef Hazan (Source: YouTube)*

### *Pulse Advertise*

The company Pulse Advertise is associated with the domain *pulseadvertise[.]com*, which was hosted on the IP address *173[.]236[.]243[.]198* from March 16, 2024, and remains active on that address at the time of writing. Similar to PULSE FZCO, Pulse Advertise is registered in the DIFZA in the United Arab Emirates. Insikt Group assesses that Pulse Advertise is potentially involved in an attack vector known as "Aladdin," which is examined in greater detail in the section titled **Companies Linked to "Czech Cluster" Potentially Linked to AdInt**.

Notably, the contact number listed for Pulse Advertise (see **Figure 10**) matches the one associated with Hadastech s.r.o., a company that, according to a Greek police report, had received payments from Intellexa for unspecified services and had imported 40 shipments from an unidentified Ukrainian company between 2020 and 2021, described as mobile phones and "other networking apparatus."

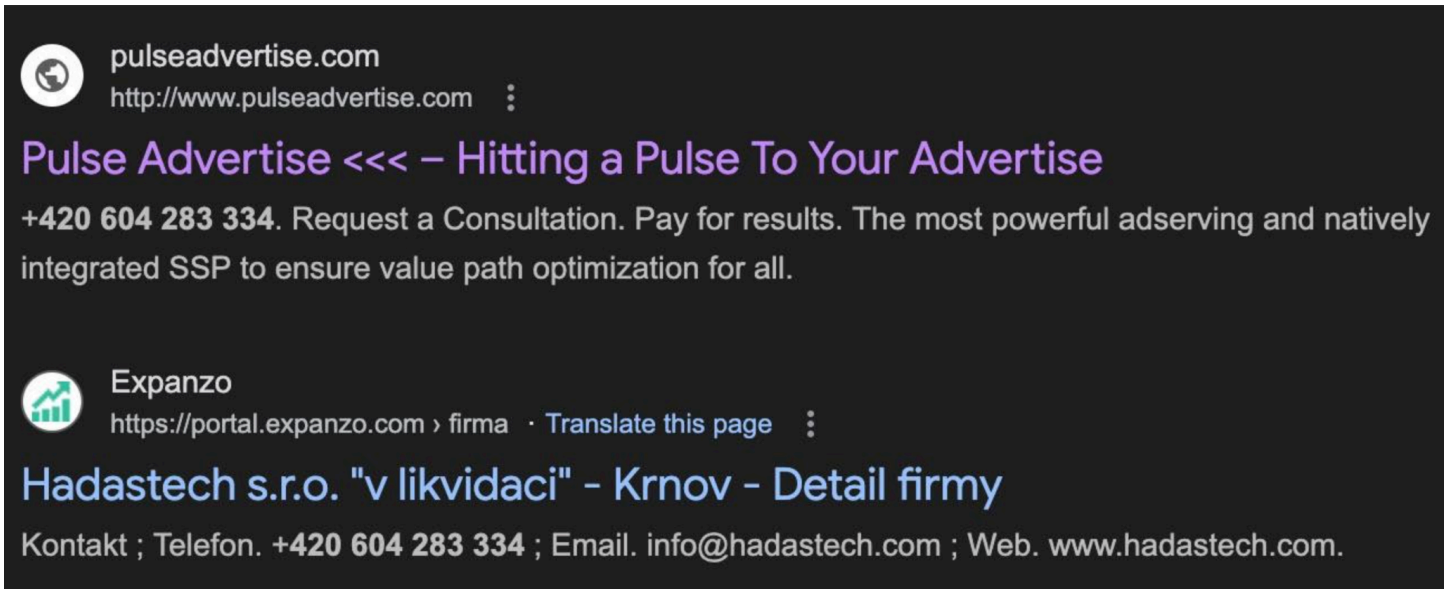


***Figure 10**: Pulse Advertise results from a Google search (Source: Google Search)*

### *MorningStar TEC*

Lastly, Insikt Group identified another company, MorningStar TEC, which is associated with the domain *morningstartec[.]com*, which was hosted on the IP address *173[.]236[.]243[.]198* from at least March 8, 2024, until the time of writing. Notably, the domain *zelus-analytics[.]com*, mentioned earlier, began resolving on the same day. According to its website, MorningStar TEC is a "Middle eastern [sic] based growth agency," specialized in "results driven marketing campaigns by leveraging creativity, technology, and bundling complimentary products for your customers" (see **Figure 11**).

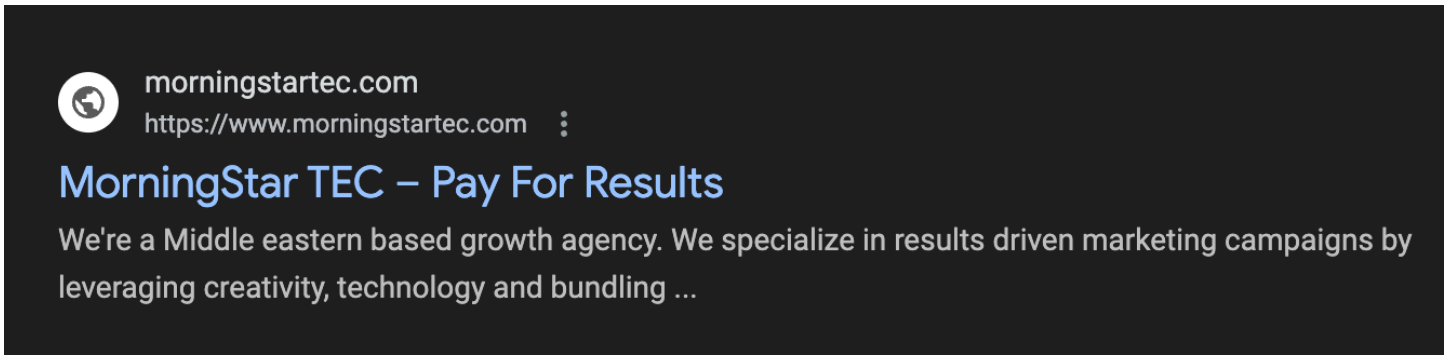


***Figure 11**: MorningStar TEC result from a Google search (Source: Google Search)*

Levi Amos (spelling may vary), an Israeli entrepreneur, is listed as the director of MorningStar TEC. He has been previously mentioned in connection with Intellexa. According to a report by the Czech investigative outlet Investigace.cz, a December 2020 shipping declaration showed that an Israeli company named Amos Levy Consultant Ltd, also referred to as Amos Levi Ltd on some documents, supplied Intellexa S.A. in Greece with "18 pallets of computer parts." The shipment reportedly followed a procurement by Hadastech s.r.o., the company linked to Dvir Horef Hazan. MorningStar TEC is linked to

Shilo s.r.o., a company associated with the domain *shilo[.]eu*, which Insikt Group had previously reported on in connection with Predator's Tier 5 infrastructure.

Similar to Pulse Advertise, Insikt Group assesses that Morning Star Tec may also be involved in an attack vector known as "Aladdin," which is discussed in greater detail in the sections below.

## Companies Linked to "Czech Cluster" Potentially Linked to Infection Vector

As noted earlier, two companies, Pulse Advertise and MorningStar TEC, stood out, as both appeared to operate in the advertising sector based on their websites. According to its website, Pulse Advertise offers "the most powerful ad-serving and natively integrated SSP [supply-side platform] to ensure value path optimization for all" (see **Figure 12**).

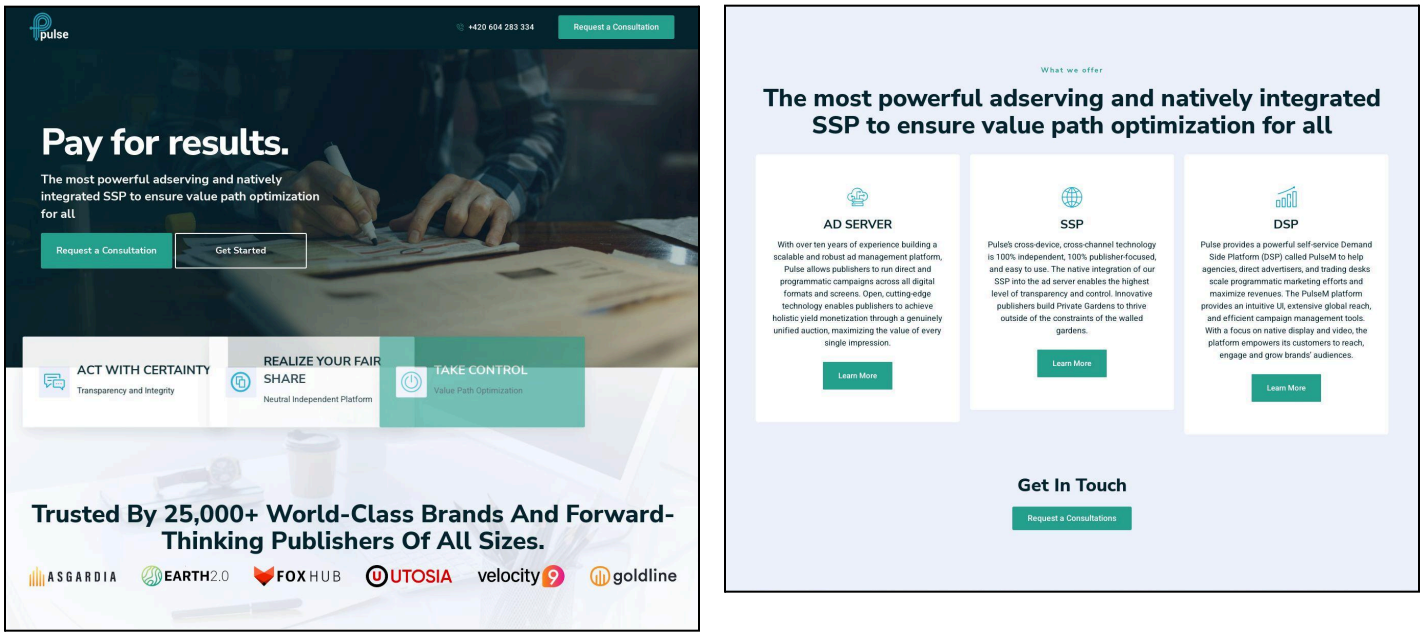


***Figure 12**: Website linked to MorningStar TEC (Source: Recorded Future)*

In turn, MorningStar TEC's business model is said to focus on performance-based outcomes rather than traditional advertising (see **Figure 13**). Notably, certain parts of MorningStar TEC's website appear to be improperly programmed; for instance, clicking on the "Benefits" tab triggers a download of the website's HTML file.

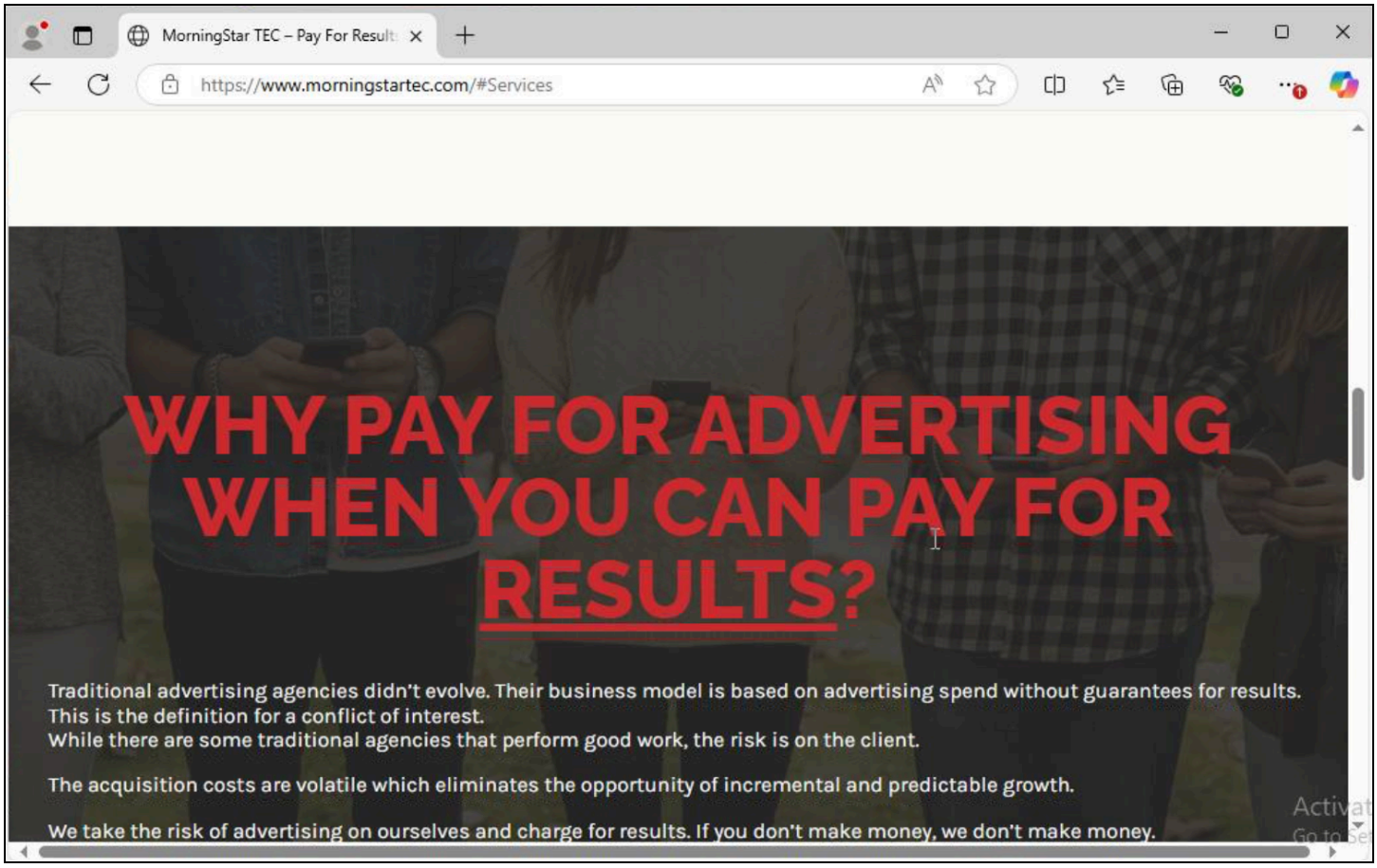


***Figure 13**: Website on* morningstartec[.]com *(Source: Recorded Future)*

Insikt Group assesses that these entities may be involved in an ad-based infection vector, specifically one referred to as "Aladdin." "Aladdin" was first reported by Haaretz in April 2024, based on leaked internal Intellexa documents from 2022. These documents described a proof-of-concept system named "Aladdin," designed to enable operators to infect targeted iOS and Android devices through malicious online advertisements. The ads, placed or directed toward specific victims, served as the delivery mechanism for the exploit. The leaked materials included demonstrations and technical documentation illustrating how the system leveraged ad networks for targeting, as well as examples of bait advertisements (such as fake job postings aimed at graphic designers or activists) that, when interacted with, would trigger the exploit chain resulting in spyware installation. "Aladdin" resembles Sherlock, a commercial surveillance capability developed by the Israeli software maker Insanet that is capable of infecting devices running Windows, Android, and iOS. Insikt Group is not aware of any reporting indicating that "Aladdin" has been used in the wild.

At a high level, the concept operates as follows: When a potential victim visits a website containing an ad slot, the site requests an advertisement from a supply-side platform (SSP). The ad exchange then solicits bids from various demand-side platforms (DSPs), which respond with bids based on their targeting parameters. The ad exchange selects the highest bid and serves the winning advertisement's

content to the website. The primary challenge in this process lies in accurately identifying the intended target and successfully winning the ad auction to ensure the malicious content is delivered to that individual.

Notably, a Vsquare report from August 2025 references an invoice dated July 28, 2022, issued to one of Dvir Horef Hazan's companies, which includes the line item "Payment for project POC, 'Aladin.'" This project is believed to be connected to the Intellexa proof-of-concept (PoC) described by Haaretz in 2024. This suggests that the Czech cluster likely played a role in "Aladdin," though the exact nature of its involvement remains unclear. It is worth noting that the name appears spelled as "Aladin" in the invoice.

## Tracing Previously Identified Intellexa Customers through Export Data

As noted above, at least one of the previously listed companies, PULSE FZCO, likely operates as a front entity used to facilitate the shipment of Intellexa-related products, either directly to suspected Intellexa customers previously identified by Insikt Group or to intermediary entities that import such products on behalf of the end customers.

### *Botswana*

Based on import records, Insikt Group identified that PULSE FZCO shipped products to Botswana's Directorate of Intelligence and Security (DIS) in October 2023. Notably, this department has previously been linked to the import of other surveillance-related products. The shipments were described in relatively generic technical terms. While the reported shipment value appears relatively low, this may reflect incomplete data in import databases, the involvement of additional front entities, or the nature of the goods themselves (for example, specific system components rather than full platforms). Notably, approximately one month after this shipment was recorded, Insikt Group observed the start of activity associated with the Predator cluster in Botswana (see **Figure 14**).

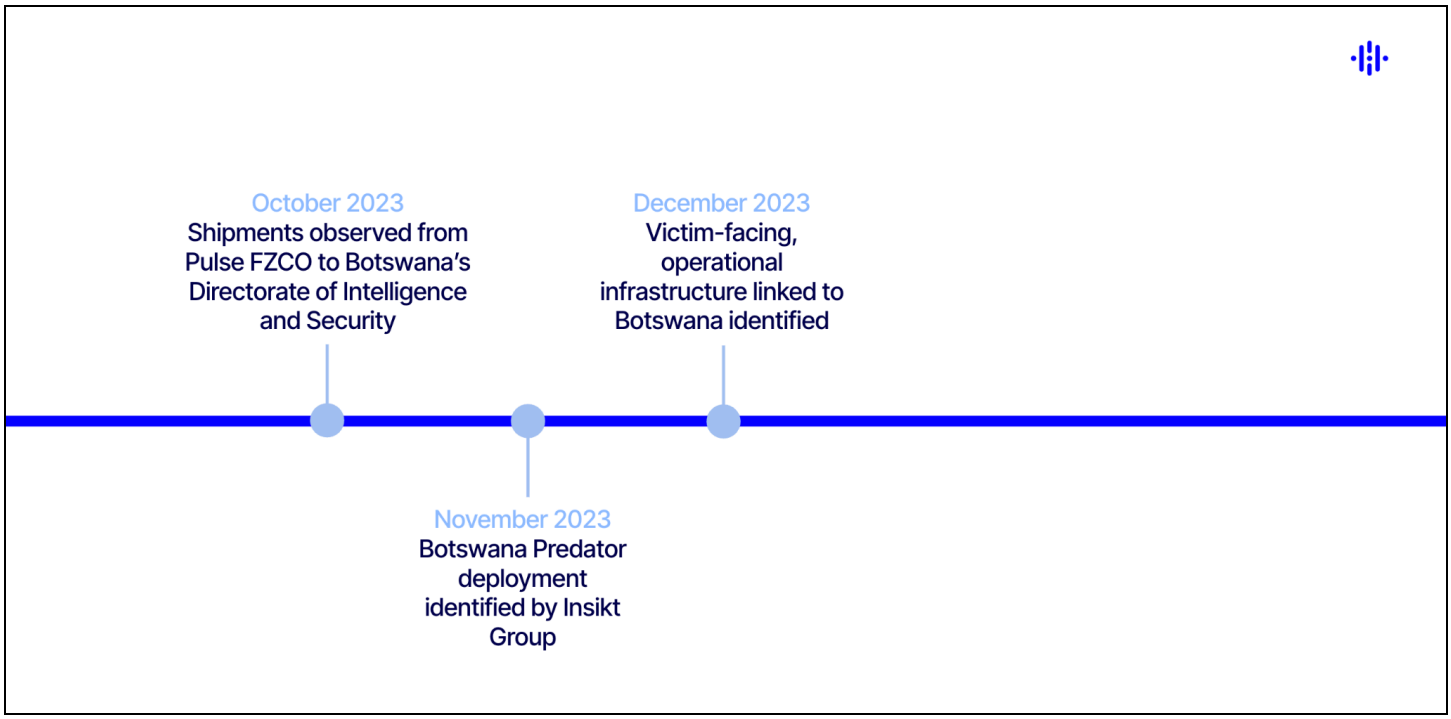


***Figure 14**: Timeline of Predator-linked activity in Botswana (Source: Recorded Future)*

Based on infrastructure analysis, Insikt Group assesses that Botswana continued to use Predator spyware at least until June 2025, and that it potentially still uses Predator at the time of writing.

### *Kazakhstan*

In October 2023, PULSE FZCO shipped products to the Kazakh company OOO Seven Hills (see **Figure 15**), with the shipment valued at approximately 6,463,070,090 KZT (around $12.4 million USD). The product descriptions are technical in nature, encompassing both software and hardware, but remain relatively generic (for example, "ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС 'АНАЛИЗ ДАННЫХ,'" which translates to "hardware-software complex 'Data Analysis'"). The company has previously been associated with the import of surveillance technologies on behalf of Kazakhstan. For instance, OOO Seven Hills was reportedly involved in importing products linked to the Swiss firm NeoSoft, which has been implicated in multiple international mobile subscriber identity (IMSI) catcher–related scandals and has allegedly sold or attempted to sell surveillance tools to repressive regimes.

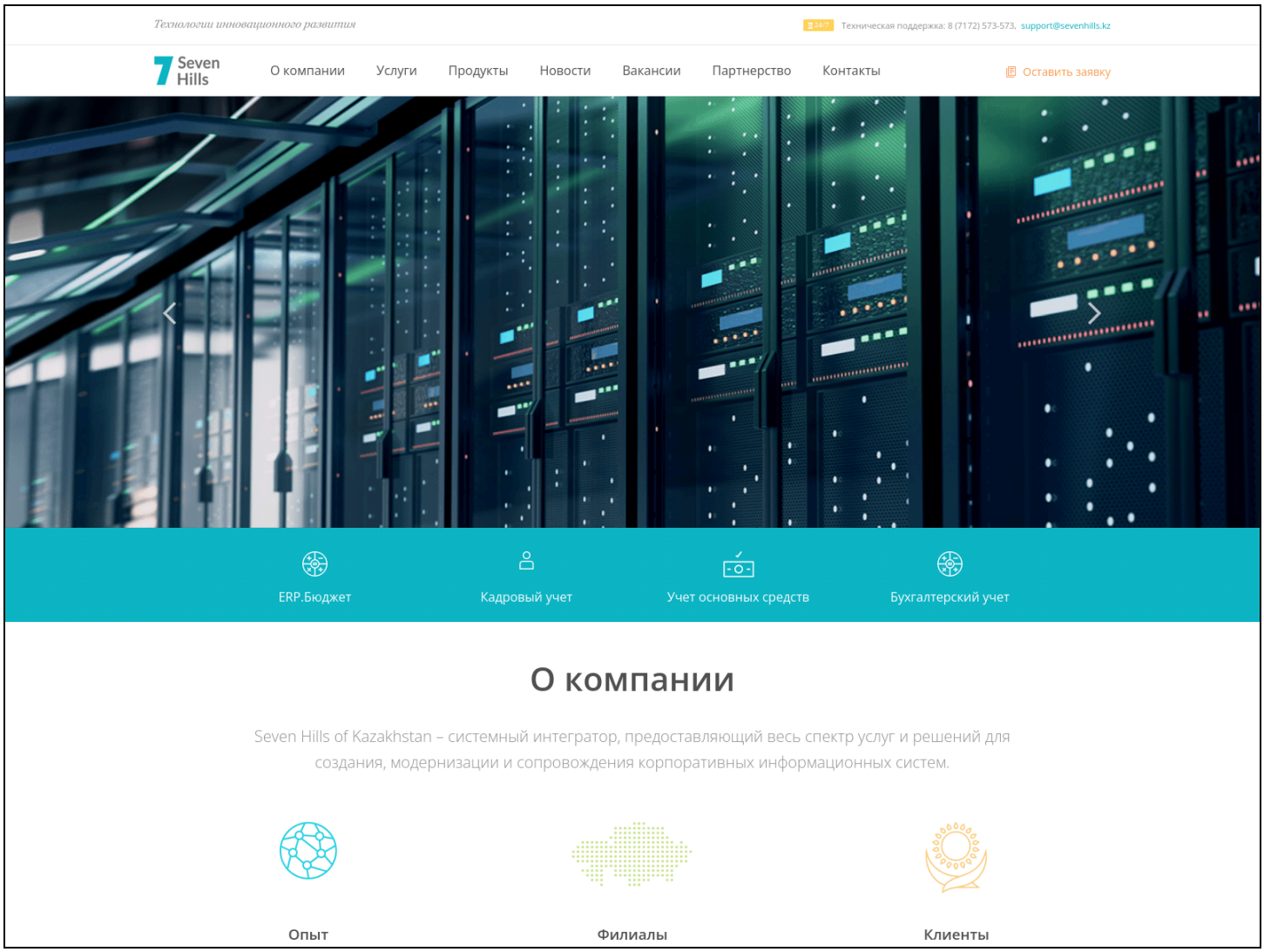


***Figure 15**: Website linked to OOO Seven Hills (Source: Recorded Future)*

Kazakhstan has been identified as a Predator user in late 2023 and was publicly reported on by Insikt Group in February 2024. The country has a track record of using cyber surveillance vendors such as NSO Group, FinFisher, and RCS Lab to target activists and politicians.

Based on infrastructure analysis, Insikt Group assesses that Kazakhstan has, at least until August 2025, continued to use Predator spyware.

### *Philippines*

In September 2023, PULSE FZCO shipped products valued at approximately $113,532 USD to the Philippines-based company ComWorks. The company is associated with the domain *comworks-inc[.]com*, and according to its website, it provides "diverse mobile solutions to different

markets that add value to our partners and principals" (see **Figure 16**). As of 2018, ComWorks was listed among the top 1,000 companies in the Philippines.


***Figure 16**: Website linked to ComWorks (Source: URLScan)*

Notably, the CEO of ComWorks holds the same position at Neo-Tech Asia Distribution, and Insikt Group further identified overlapping employees as well as signs of a potential reselling collaboration.

Insikt Group previously identified a Predator customer assessed to be highly likely linked to the Philippines in 2023 and publicly reported on this finding in February 2024. It remains unclear whether this Predator customer continues to be active at the time of writing.

## Ongoing Intellexa Operations Across Multiple Countries

Following various publications on Intellexa's Predator infrastructure since 2023 by Insikt Group and others, Intellexa started changing its infrastructure setups making some forms of detection harder, as we anticipated. For example, while Insikt Group is still observing domains hosted on virtual private servers, there has been a push towards hiding the infrastructure behind Cloudflare. Overall, Insikt Group has observed less infrastructure in 2025 than in 2024, suggesting that activity has slowed, with changes in domain naming conventions making it harder to connect domains to specific regions and, thereby, customers.

Overall, this makes it more difficult to assess the level of activity associated with the observed Predator clusters. Using Recorded Future Network Intelligence, Insikt Group determined that the Mozambique-linked cluster, previously reported, remained active through at least late June 2025.

Furthermore, several Tier 4 servers in other clusters tied to Predator spyware customers continued to communicate with the Tier 5 infrastructure (see **Figure 18**). As of writing, customers assessed to be based in Saudi Arabia, Kazakhstan, Angola, and Mongolia were still observed communicating with Tier 5 infrastructure, suggesting continued activity. In contrast, customers in Botswana, Trinidad and Tobago, and Egypt ceased communication in June, May, and March 2025, respectively. This may indicate that these entities discontinued their use of Predator spyware around those times; however, it is also possible that they merely modified or migrated their infrastructure setups.

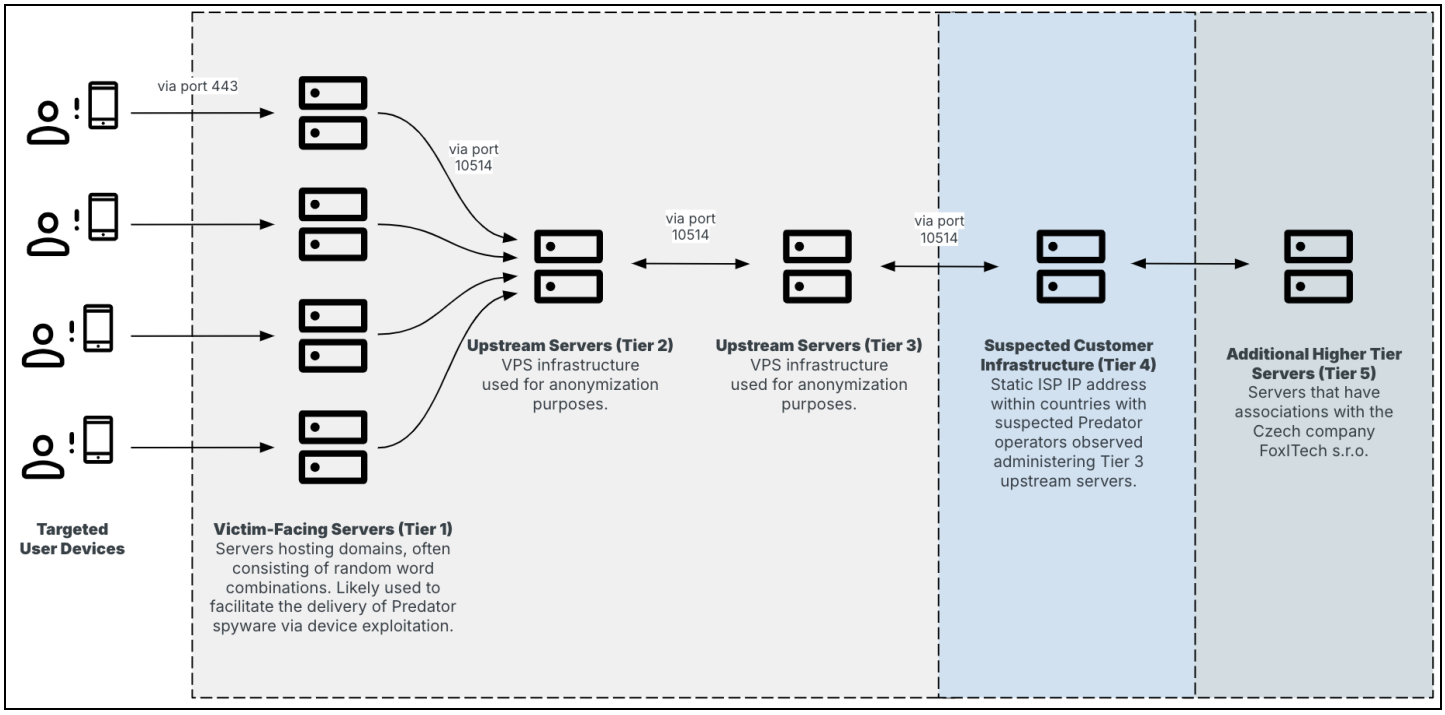


***Figure 18**: Multi-tiered infrastructure linked to Predator (Source: Recorded Future)*

### *Additional Evidence Supports Operational Presence in Iraq*

Insikt Group previously observed that Predator-related domains often included keywords or naming patterns that could offer insight into their targeting or associated customers. Drawing on this observation, and in combination with Recorded Future Network Intelligence, Insikt Group had, for instance, historically assessed Predator activity in Iraq, identifying multiple domains likely referring to communities or groups linked to the Badini dialect spoken in the Badinan region of Iraqi Kurdistan. Notably, the first and fourth domains became active on the same day, while the second and third domains also appeared to have gone live around the same time. "Gardalul" is a documentary exploring the history of Kurds in Iraqi Kurdistan and the lives of the Peshmerga fighters during the Ba'ath regime.

| Domain | IP Address | First Seen | Last Seen |
|---|---|---|---|
| badinigroup[.]com | 38[.]180[.]54[.]77 | 2024-01-31 | 2025-01-22 |
| keep-badinigroups[.]com | 5[.]253[.]43[.]92 | 2024-07-01 | 2025-07-01 |
| gardalul[.]com | 45[.]86[.]231[.]8 | 2024-07-02 | 2025-06-29 |
| birura[.]com | 89[.]150[.]57[.]85 | 2024-01-31 | 2025-01-24 |

***Table 1**: Domains and IP addresses likely linked to a Predator customer located in Iraq (Source: Recorded Future)*

More specifically, Insikt Group observed network communications between the Tier 5 infrastructure, described in greater detail in Insikt Group's June 2025 report on Predator, and a static internet service provider (ISP)-assigned IP address geolocated in Iraq. The communication pattern matched that typically observed between Tier 4 servers and Tier 5 infrastructure in other Predator deployments.

In addition, Insikt Group identified suspected victim traffic originating from Iraqi IP space to at least one Predator Tier 1 server, specifically *169[.]239[.]129[.]23*, which hosted the domain *eppointment[.]io* on April 8, 2024. Although Insikt Group has not yet observed a complete communication chain linking Tier 1 through Tier 5, Insikt Group assesses with medium confidence that there is a Predator spyware customer located in Iraq, and that this customer likely remains operational in 2025.

For context, Iraqi authorities, specifically the Counter-Terrorism Service (CTS), previously sought to procure Hacking Team's "RCS/Galileo" spyware around 2014 and 2015, as revealed through leaked correspondence in which an "Iraq government representative" requested to "test" the company's phone-hacking solution, suggesting a direct procurement attempt. A leaked client renewal spreadsheet also listed "INTECH-CONDOR K — Iraqi Kurdistan" as active (renewal dated June 30, 2015), indicating an operational deployment in the Kurdistan Region of Iraq (KRI) via a reseller. Supporting this, German media reported that spyware had been supplied to Kurdish authorities in northern Iraq under the codename "Condor." The government of Kurdistan has also been linked to other spyware sales, such as through the intermediary Ben Jamil.

### *Suspected Activity in Pakistan*

Insikt Group identified infrastructure indicators likely associated with the use of Predator spyware linked to Pakistan. However, based on the identified indicators, it remains unclear whether these were deployed against targets within or connected to Pakistan, or whether a customer was operating from Pakistan. Based on the identified infrastructure indicators, Insikt Group assesses that the targeting likely focused on individuals located in or connected to the Balochistan region.

## Mitigations

- Leverage indicators of compromise (IoCs) to identify potential past or ongoing infections and use the Recorded Future® Intelligence Cloud to monitor for Predator or other malware.
- Adopt a collective security mindset by remaining vigilant about both your own exposure and that of colleagues, friends, and family who may be targeted indirectly.
- Exercise heightened caution toward spearphishing attempts, verifying unexpected messages or attachments before engaging with them.
- Limit the use of unnecessary applications to reduce your device's attack surface and minimize exposure to malicious or compromised software.
- Keep mobile devices fully updated by promptly applying operating system and app patches to mitigate known security vulnerabilities.
- Enable Lockdown Mode where available to strengthen device defenses against advanced spyware and exploit-based attacks.
- Use ad-blocking and restrict ad-tracking identifiers to reduce exposure through malicious advertising and tracking-based attack vectors.

## Outlook

Insikt Group's latest research provides a deeper look into Intellexa's corporate network, revealing a web of interconnected entities that likely serve distinct operational purposes. Despite mounting public exposure and international measures intended to limit its proliferation, Intellexa remains active, illustrating how resilient and adaptable the mercenary spyware industry has become. The findings also highlight that tracking and analyzing advanced spyware like Predator is increasingly complex, not only due to evolving exploit and delivery techniques but also because of the opaque global corporate structures that enable and obscure such operations. This comes with a broader proliferation of such capabilities making once-exclusive offensive technologies far more widely available. In an era of global fragmentation, conflict, and power shifts, demand for these capabilities continues to grow, as intelligence on individuals' activities, thoughts, and creations becomes an instrument of political, economic, and social control.

Looking ahead, while not comprehensive, Insikt Group assesses that several key patterns are shaping the trajectory of the spyware ecosystem. A process of balkanisation is clearly underway, with companies increasingly dividing along geopolitical lines: Some previously sanctioned entities are

seeking legitimacy and access to Western markets through acquisitions (1, 2), while others are turning toward regions with less oversight. This fragmentation is accompanied by constant market turnover, as newly established or rebranded firms emerge to replace sanctioned or defunct entities, often functioning as fronts or continuations of the same underlying operations, making corporate and legal analysis increasingly critical for effective threat research. Despite these shifts, a core set of individuals and facilitators remains persistent, reappearing across different companies and serving as the enduring legal, financial, and logistical backbone of the industry. Meanwhile, industry challenges are intensifying: The high value of spyware technologies, particularly their exploit capabilities, and the secrecy surrounding them fuel risks of corruption, insider leaks, and even attacks on the mercenary spyware companies themselves. Finally, the scope of targeting continues to widen beyond journalists, activists, and politicians to include corporate leaders and private-sector figures, as evidenced by cases involving Predator in Greece and Paragon in Italy (1, 2). These developments suggest that what is publicly visible likely represents only a small portion of a much larger and largely concealed global ecosystem. An often underreported aspect is the high personal and professional cost victims face when speaking out, as doing so can jeopardize business relationships, sourcing opportunities (for example, in journalism), or trust (such as within the security community).

Together, these dynamics suggest a continuing evolution and diffusion of mercenary spyware operations, requiring sustained scrutiny, coordinated policy efforts, and improved technological and legal countermeasures to mitigate their global impact.

## Appendix A: Indicators of Compromise (IoCs)

**Domains:**
badinigroup[.]com
birura[.]com
gardalul[.]com
keep-badinigroups[.]com

**IP Addresses:**
5[.]253[.]43[.]92
38[.]180[.]54[.]77
45[.]86[.]231[.]8
89[.]150[.]57[.]85

## Appendix B: MITRE ATT&CK Techniques

| Tactic: Technique | ATT&CK Code |
|---|---|
| **Resource Development:** Acquire Infrastructure: Domains | T1583.001 |
| **Resource Development:** Acquire Infrastructure: Virtual Private Server | T1583.003 |
| **Resource Development:** Acquire Infrastructure: Server | T1583.004 |
| **Initial Access**: Spearphishing Link | T1566.002 |
| **Execution:** Exploitation for Client Execution | T1203 |

*Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.*

## *About Insikt Group®*

*Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.*

## *About Recorded Future®*

*Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.*

*Learn more at recordedfuture.com*