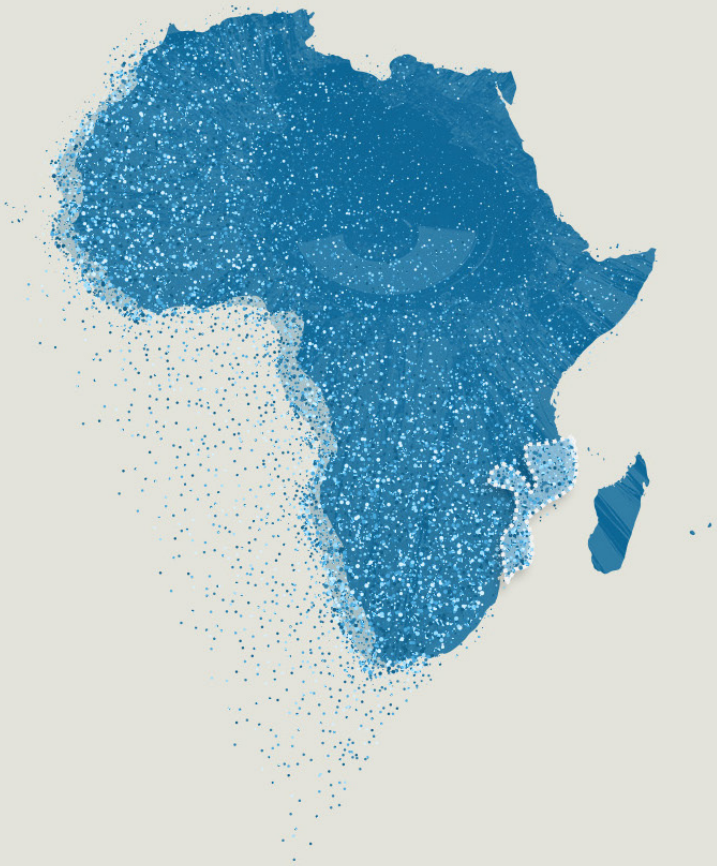
CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

June 12, 2025



Predator Still Active, with New Client and Corporate Links Identified

Insikt Group has identified new infrastructure linked to Predator, indicating continued operations despite public exposure, sanctions, and policy interventions such as the Pall Mall Process.

Insikt Group has observed Predator-linked activity across multiple countries over the past year and is the first to report a suspected Predator operator presence in Mozambique.

Insikt Group linked components of Predator's infrastructure to a Czech entity that had been previously associated with the Intellexa Consortium by an investigative media outlet.

Executive Summary

Following major public exposures by Insikt Group and others throughout the last two years, alongside US government sanctions targeting the Intellexa Consortium — the organizational structure behind the Predator mobile spyware — Insikt Group observed a significant decline in Predator-related activity. This apparent decline raised questions about whether the combination of US sanctions, public exposure, and broader international efforts to curb spyware proliferation, such as the UK and France-led Pall Mall process, had dealt a lasting blow to Intellexa's operations. Yet, Predator activity has not stopped, and in recent months, Insikt Group has observed a resurgence of activity, reflecting the operators' continued persistence. While much of the identified infrastructure is tied to known Predator operators in countries previously identified by Insikt Group, a new customer has also been identified in Mozambique — a country not previously publicly linked to the spyware. This aligns with the broader observation that Predator is highly active in Africa, with over half of its identified customers located on the continent. Additionally, Insikt Group has found a connection between high-tier Predator infrastructure and a Czech entity previously associated with the Intellexa Consortium.

The deployment of spyware like Predator beyond legitimate criminal or counterterrorism use poses serious threats to privacy, legal rights, and the physical safety of both direct targets and associated individuals. While most known cases of abuse have targeted civil society and political activists, individuals and organizations in regions with a record of spyware misuse should remain vigilant, regardless of sector. Given Predator's expensive licensing model, its use is typically reserved for high-value, strategic targets. This makes politicians, corporate executives, and others in sensitive positions especially vulnerable due to the intelligence they may possess. The use of spyware against political opposition figures is currently under investigation in several EU countries, reflecting wider global efforts to curb the activities of mercenary spyware developers.

As outlined in Insikt Group's previous reports on Predator, defenders should follow recommended best practices. These include ensuring personal and corporate devices are kept separate, regularly updating phones, encouraging periodic device reboots (though this may not always fully eliminate Predator), using lockdown mode, and implementing a mobile device management (MDM) system. Additionally, investing in security awareness training for employees and fostering a culture of minimal data exposure are essential for reducing the risk of successful spearphishing attacks and limiting data theft in the event of a breach.

Insikt Group expects the mercenary spyware market to continue expanding, fueled by sustained demand and corporate profitability. This growth will likely be accompanied by ongoing innovation, as rising competition and strengthened IT security among targets drive the development of new products and techniques. For instance, as defenders work to eliminate entire classes of vulnerabilities, spyware operators may adapt by targeting alternatives such as cloud backups accessed via stolen credentials or by employing new deployment methods. As these tools proliferate and techniques evolve, the range of victims is likely to extend beyond civil society, influencing political discourse and sparking further legal confrontations. Recent court rulings in favor of technology companies against spyware vendors may set

a precedent, encouraging more firms to actively challenge the misuse of their platforms. Insikt Group anticipates that spyware vendors will continue leveraging complex corporate structures to evade sanctions or detection, while increasingly tailoring their operations to specific regions, a trend often described as the balkanization of the ecosystem.

Key Findings

- Insikt Group has identified new infrastructure associated with Predator, indicating continued operations despite public exposure, international sanctions, and policy interventions.
- The newly identified infrastructure includes both victim-facing Tier 1 servers as well as high-tier components that likely link back to Predator operators in various countries.
- Although much of Predator's infrastructure remains consistent with previous reporting, its operators have introduced changes designed to further evade detection — a pattern Insikt Group noted in earlier reporting.
- Insikt Group has detected Predator-related activity in several countries throughout the last twelve months and is the first to report a suspected Predator operator presence in Mozambique.
- Insikt Group also connected components of Predator's infrastructure to a Czech entity previously linked with the Intellexa Consortium by a Czech investigative outlet.

Background

Predator is a sophisticated mercenary spyware targeting both Android and iPhone devices and has been active since at least 2019. Originally developed by Cytrox and now operated under the Intellexa alliance,[1] Predator is engineered for flexibility and stealth, leaving minimal evidence on infected devices and making external investigations into abuse particularly challenging. Once deployed, Predator provides complete access to a device's microphone, camera, and all data — such as contacts, messages, photos, and videos — without the victim's awareness. The spyware's modular design, based on Python, allows operators to introduce new features remotely, without the need to re-exploit the device.

Predator can be delivered through both "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).

[1] Formed in 2019, the Intellexa alliance is a technological and commercial collaboration between the Intellexa and Nexa groups. With separate shareholdings, the alliance comprises companies such as Nexa Technologies, Advanced Middle East Systems, Cytrox, WiSpear, and Senpai Technologies, as announced in a press release. The current status of this alliance remains unclear.

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). Notably, this is the first public report to identify Mozambique as a suspected customer. While Predator is ostensibly marketed for counterterrorism and law enforcement purposes, previous reporting has documented a clear pattern of its deployment against civil society actors, including journalists and activists, and politicians (1, 2, 3, 4). These instances described in earlier reports likely represent only a small portion of the overall abuses, given the widespread use of mercenary spyware like Predator, the difficulty of detection, and limited victim support. It is important to emphasize the risk of cross-border targeting, which has been observed not only with Predator, where an operator linked to Vietnam has targeted EU officials and members of the European Parliament, but also with other mercenary spyware, such as Pegasus.

Despite increased public reporting on Predator's infrastructure and techniques, as well as growing attention to Intellexa's corporate structure, Predator operations remain active. 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[2], alongside likely rising exploit costs, particularly for iPhones. This likely reflects growing demand for spyware tools, especially in countries facing export restrictions, ongoing technical innovation in response to public reporting and security enhancements, and increasingly complex corporate structures designed to impede sanctions and attribution. One such example, involving a Czech entity likely linked to Predator operations, is discussed later in this report.

Threat Analysis

Tier 1 (C2) Servers

Insikt Group has identified new victim-facing Tier 1 (C2) infrastructure that is highly likely associated with Predator, including domains and IP addresses. Although the specific functions of these domains and IP addresses have not yet been confirmed, they are probably involved in payload delivery and the exploitation process, consistent with previous infrastructure linked to Predator. A table in **Appendix B** presents the domains and IP addresses observed over the past twelve months.

Previously, domains linked to Predator often impersonated specific organizations, such as frequently visited local news outlets, as Insikt Group has reported in the past (1, 2). However, this pattern began to gradually shift following increased media attention and public reporting from the end of 2023 onward. More recent domains now typically consist of two or more seemingly random English words. Insikt Group has observed that some of these domains reuse particular keywords; for instance, both *boundbreeze[.]com* and *branchbreeze[.]com* share the word "breeze". In a few recent cases, domains feature Portuguese-language words, which likely reflect the language of intended targets. Additionally, certain domains contain keywords that could provide clues to their targeting, such as

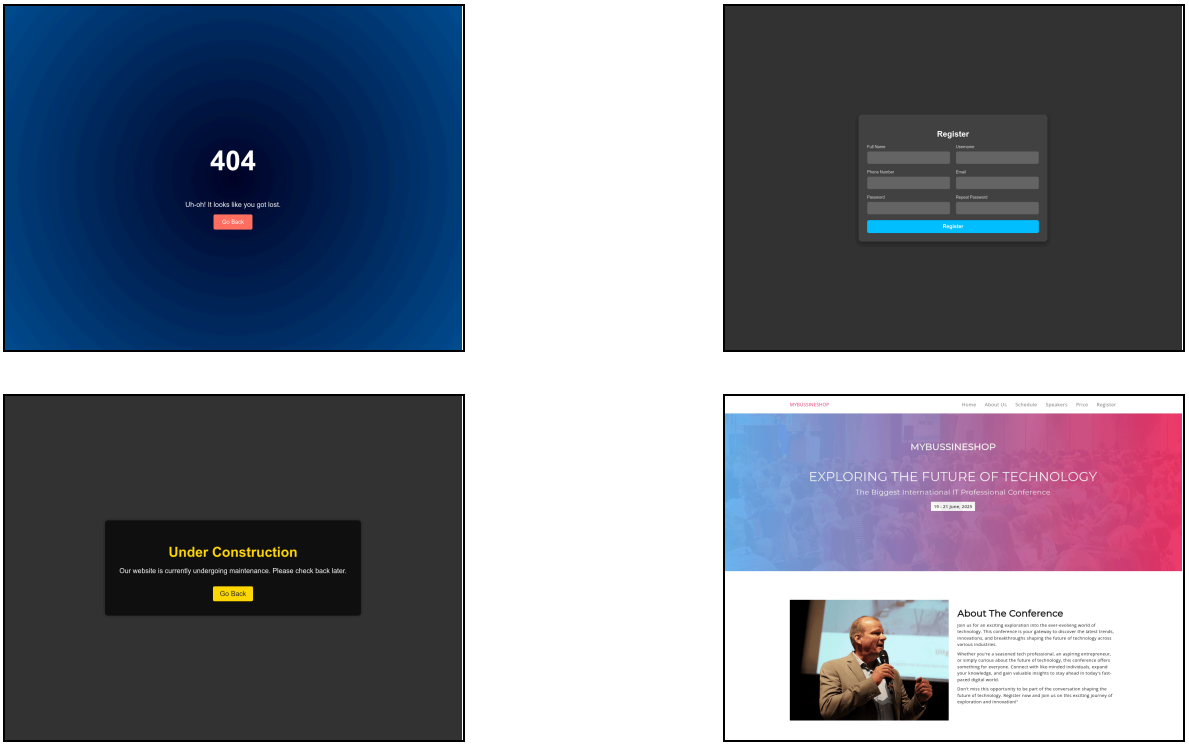
[2] The Pall Mall Process is an initiative launched by the governments of France and the United Kingdom, aimed at establishing standards for the ethical use of commercially available technologies in intrusive surveillance operations.

keep-badinigroups[.]com, which may refer to communities or groups associated with the Badini dialect spoken in the Badinan region of Iraqi Kurdistan.

The majority of identified domains have been registered through the registrar PDR Ltd. d/b/a PublicDomainRegistry.com and typically use name servers associated with *orderbox-dns[.]com*, among others. While Predator infrastructure has historically favored certain autonomous system numbers (ASNs) such as AS62005, AS61138, and AS44066, Insikt Group has observed that more recent Predator-linked domains are being hosted on a broader range of ASNs — including AS42708, AS20473, and AS44477 — which have not previously been connected to Predator activity. Notably, Insikt Group also identified at least one instance where a server tied to higher-tier Predator infrastructure was hosted with Stark Industries.

Suspected Infrastructure Detection Evasion Strategies

In response to ongoing public exposure, the operators behind Predator have adopted various tactics to evade detection. These involve using more varied server configurations than previously reported, expanding the diversity of ASNs, and introducing additional layers to their multi-tiered infrastructure, among other approaches. One notable strategy involves the use of fake websites, which generally fall into four main categories: fake 404 error pages, counterfeit login or registration pages, sites indicating that they are under construction, and websites purporting to be associated with specific entities, such as a conference (see **Figures 1-4**).



***Figures 1-4**: Example websites linked to Predator (Source: Recorded Future)*

Notably, websites associated with Predator have been found on either a single server or a small number of Predator-controlled servers.

Multi-Tiered Infrastructure

As previously reported by Insikt Group, Predator customers continue to use a multi-tiered infrastructure network, which is likely designed to enable the targeting of specific individuals or entities (see **Figure 5**). This network closely resembles the high-level architecture outlined in Amnesty's October 2023 report, but it has continued to evolve since then. Earlier versions of Predator's multi-tiered infrastructure, reported by Insikt Group in March 2024, featured only three layers. The addition of a fourth layer in the current design is likely intended to further obscure the identification of countries suspected of deploying Predator.

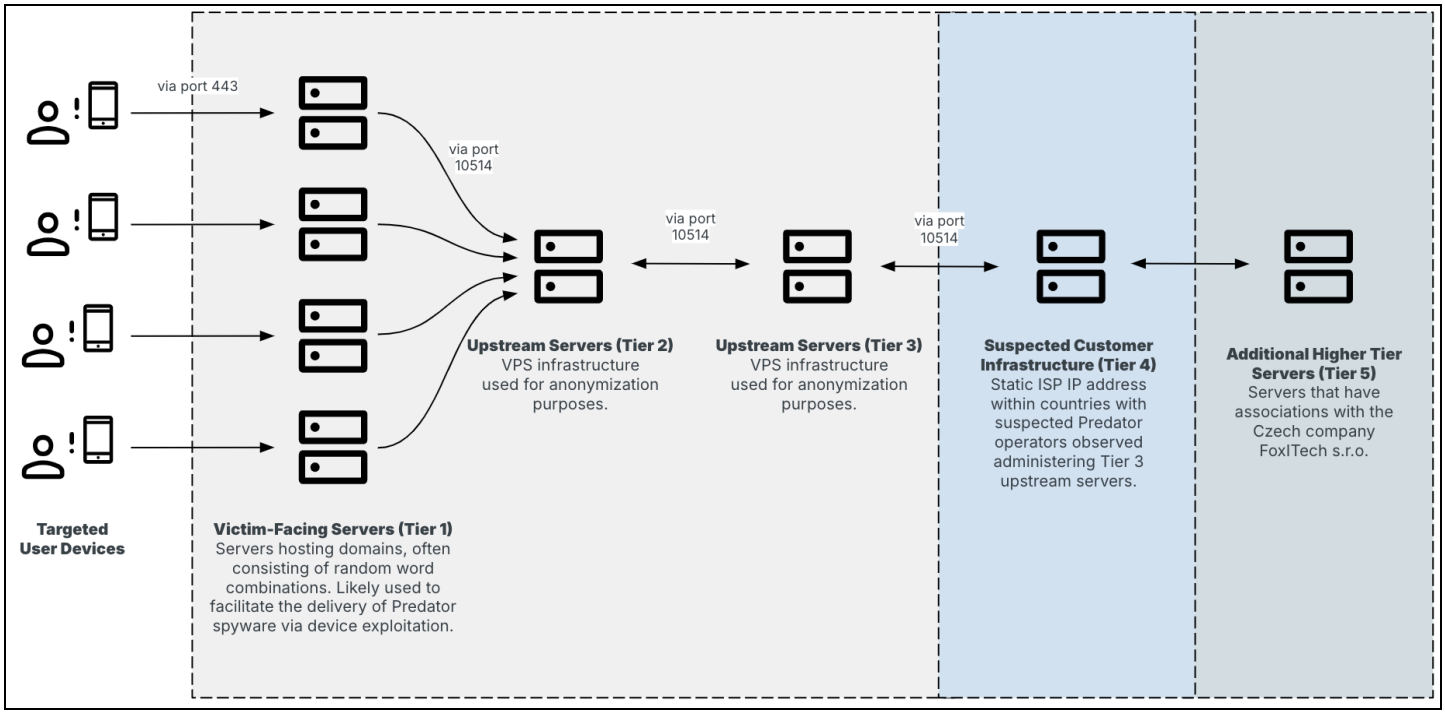


***Figure 5**: Multi-tiered infrastructure linked to Predator (Source: Recorded Future)*

Leveraging Recorded Future® Network Intelligence, Insikt Group has observed that Tier 1 servers consistently communicate with a dedicated Tier 2 upstream virtual private server (VPS) IP address using Transmission Control Protocol (TCP) port 10514. These upstream servers likely function as anonymization hop points, making it more difficult to associate Tier 1 servers directly with individual Predator customers. Communication over TCP port 10514 is also consistently observed between Tier 2 and Tier 3 servers. Subsequently, Tier 3 servers relay traffic to the Tier 4 layer, which appears to correspond to static, in-country ISP IP addresses suspected to be under the control of Predator customers. In every instance analyzed, both the Tier 1 servers and their corresponding upstream servers appeared to be dedicated exclusively to a single customer.

While only Tiers 1 through 4 appear directly connected to the operational infrastructure of Predator customers, Insikt Group has also been monitoring an additional layer, tracked as Tier 5, that seems to play a central, though still unclear, role in Predator-related operations. Tier 5 servers have been linked to an entity in the Czech Republic, FoxITech s.r.o., which has previously been publicly associated with Intellexa and is discussed further in the Connection to Czech Entity section.

Suspected Predator Usage Within Specific Countries

Since Insikt Group began reporting on Predator in March 2024, suspected operators of the spyware have been identified in over a dozen countries worldwide. While several of these operators have remained active in the past twelve months, activity appears to have ceased in some locations, likely due to public reporting, leading to an overall lower number of current Predator operators. For example, in the Democratic Republic of the Congo (DRC), operations seem to have stopped about two weeks after Insikt Group published its findings on DRC-linked activity in September 2024. Similarly, the suspected operator in Angola became inactive around the same period, only to resume activity in early 2025, based on Recorded Future Network Intelligence. Additionally, Insikt Group has uncovered evidence of Predator use in Mozambique — a country where no Predator operators had been identified before this report.

Mozambique

Drawing on Recorded Future Network Intelligence and other artifacts, Insikt Group attributes the domains listed in **Table 1** with high confidence to a suspected Predator operator based in Mozambique. Additionally, several other domains, including *mdundobeats[.]com*, *noticiafamosos[.]com*, and *onelifestyle24[.]com*, as well as others from **Appendix B**, are likely linked to the same customer based on various technical indicators in Recorded Future sources. Notably, all IP addresses associated with these domains, except for the one hosting *onelifestyle24[.]com*, fall within the same two /24 CIDR ranges. Insikt Group further assesses, using both Recorded Future Network Intelligence and passive DNS data, that the suspected Predator operator in Mozambique became active during the first half of 2024 and still appears to be active at the time of writing.

Domain	IP Address	Notes
canylane[.]com	169[.]239[.]128[.]42	N/A
flickerxxx[.]com	169[.]239[.]129[.]57	Potentially impersonates the legitimate online photo-sharing and hosting platform Flickr (*flickr[.]com*)
mundoautopro[.]com	169[.]239[.]128[.]48	N/A
noticiafresca[.]net	169[.]239[.]128[.]46	Likely impersonates the legitimate Mozambique-based news website of Notícias Frescas MZ (*noticiasfrescasmz[.]com*)

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

Although there has been no public reporting to date linking Predator to Mozambique, earlier investigations have connected the country to other forms of surveillance. In 2021, a report, drawing on a 2018 Citizen Lab analysis, suggested that Mozambique was likely a Pegasus operator (there were no confirmed Pegasus infections within Mozambique at that time). Additionally, a 2016 report by the Mozambican investigative outlet Verdade revealed that the government had acquired and was using advanced surveillance technologies to monitor citizens' communications.

Additional Cluster Linked to Eastern European Country

While many of the identified domains and IP addresses can be attributed to specific suspected operators in particular countries, attribution is less straightforward in other cases. Technical indicators frequently connect multiple domains and IP addresses into distinct clusters, which Insikt Group assesses are likely controlled by the same operator.

One such cluster was notable for its brief period of activity. Recorded Future Network Intelligence indicates this cluster was active only from August to November 2024 and likely consisted of just two sets of Tier 1 to Tier 4 servers. This cluster could represent testing and development operations due to its brevity, or it could be linked to an Eastern European operator on account of its location. Currently, *speedbrawse[.]com* is the sole domain associated with this cluster. Insikt Group assesses that the abrupt halt in activity of this operator may also be linked to the escalation of sanctions against Intellexa in September 2024.

Connection to Czech Entity

During the investigation into the use of Predator against the Greek journalist Thanasis Koukakis and others, Greece's Supreme Court prosecutor directed the financial police to compile a report on companies connected to the Intellexa Consortium — a document later obtained by the Czech investigative outlet Investigace.cz. This report features a supplier table listing entities associated with Intellexa, including an individual named Dvir Horef Hazan. He, along with the connections described in the report, is shown in **Figure 6**.

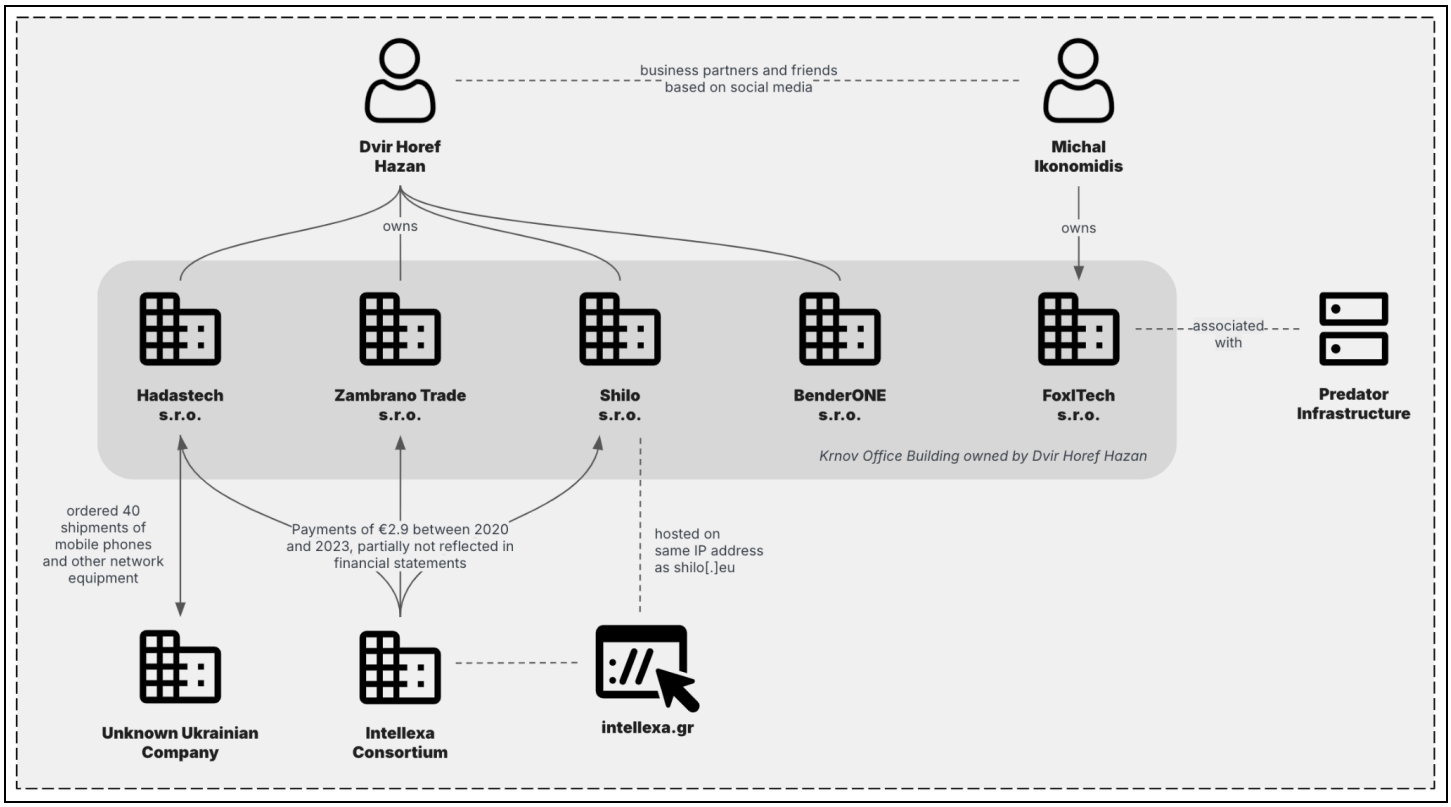


***Figure 6**: Connections between Predator infrastructure and FoxITech s.r.o. (Source: Investigace.cz, Recorded Future)*

Investigations by the Czech outlet found that Hazan, a Czech bistro owner, programmer, and entrepreneur with ownership of at least eight Czech companies, with four specializing in marketing, consulting, and IT advisory, allegedly worked for Intellexa. Greek police reports show that Intellexa transferred nearly €3 million to Hazan and three of his companies (Zambrano Trade s.r.o., Hadastech s.r.o., and Shilo s.r.o.) for unspecified services. Additionally, Importgenius records reveal that Hadastech, solely directed by Hazan, received 40 shipments from an unidentified Ukrainian company between 2020 and 2021, described as mobile phones and "other networking apparatus."

Further analysis shows that Hazan is also indirectly linked to FoxITech s.r.o., a Czech company based in Krnov and owned by Michal Ikonomidis, which claims to provide integrated IT and business services, including software development, cybersecurity, HR recruitment, and back-office support, to clients globally. More specifically, FoxITech s.r.o. is headquartered in a building owned by one of Hazan's companies, which also houses the other previously mentioned Hazan-owned businesses. This link between Hazan and FoxITech s.r.o. is further evidenced by Hazan and Ikonomidis appearing to be friends, based on social media, and the fact that Hazan's first company and FoxITech s.r.o. were both registered at the notary's office by the same proxy. Moreover, RIPE (Réseaux IP Européens) entries linked to FoxITech s.r.o. include email addresses associated with Hazan's company, Shilo s.r.o. According to Investigace.cz, an email sent to FoxITech s.r.o. was answered from an address belonging to one of Hazan's companies, Bender ONE s.r.o.

Although the precise nature and purpose of the connection between FoxITech s.r.o. and Predator operations remain unclear, Insikt Group has observed that Tier 4 servers regularly communicate with Tier 5 infrastructure, which is linked to FoxITech s.r.o. This establishes a link between Predator's multi-tiered infrastructure and the Czech entity, marking the first technical connection made between Predator infrastructure and corporate entities associated with the Intellexa Consortium.

Notably, Investigace.cz previously reported on Cytrox in the Czech Republic, revealing that the company's listed director was a pensioner from a village near Ostrava, unaware of Intellexa. She knew Hazan, a family acquaintance living nearby. Also, her daughter's husband, Amos Uzan, is an Israeli who worked in government security and communications roles from 2003–2009, during Ehud Olmert's tenure as Prime Minister. Olmert had previously disclosed that he was a paid advisor to Intellexa between 2006 to 2009.

Outlook

Insikt Group has uncovered evidence indicating the continued use of Predator, including in Mozambique, despite widespread media attention and sanctions targeting Intellexa and related entities. Although recent activity has been observed, the reduced number of suspected operators compared to earlier reports suggests that public exposure, sanctions, and related measures have likely imposed operational costs on Intellexa. Moreover, while Predator operators historically maintained a consistent modus operandi, the latest findings reveal the adoption of new tactics to evade detection. Sanctions and other pressures are likely to drive efforts to increase the complexity of corporate structures, making operations harder to trace and disrupt. The continued spread of Predator and similar spyware products, as well as the availability of hack-for-hire services beyond legitimate law enforcement and counterterrorism uses, presents a significant risk to a broad range of organizations and individuals.

Appendix A: Indicators of Compromise

Domains:

asistentcomercialonline[.]com
barbequebros[.]com
boundbreeze[.]com
branchbreeze[.]com
c3p0solutions[.]com
caddylane[.]com
canylane[.]com
clockpatcher[.]com
colabfile[.]com
craftilly[.]com
dollgoodies[.]com
drivemountain[.]com
eclipsemonitor[.]com
flickerxxx[.]com
gamestuts[.]com
gettravelright[.]com
gilfonts[.]com
gobbledgums[.]com
humansprinter[.]com
infoshoutout[.]com
keep-badinigroups[.]com
lawrdo[.]com
longtester[.]com
mappins[.]io
mdundobeats[.]com
mountinnovate[.]com
mundoautopro[.]com
myprivatedrive[.]net
myread[.]io
mystudyup[.]com
nightskyco[.]com
noticiafamosos[.]com
noticiafresca[.]net
onelifestyle24[.]com
openstreetpro[.]com
pedalmastery[.]com
pinnedplace[.]com
remixspot[.]com
roadsidefoodie[.]com
secneed[.]com
secsafty[.]com
shopstodrop[.]com
speedbrawse[.]com
stableconnect[.]net
starryedge[.]com
statuepops[.]com
steepmatch[.]com
streamable-vid[.]com

strictplace[.]com
svcsync[.]com
themastersphere[.]com
traillites[.]com
trigship[.]com
unibilateral[.]com
updatepoints[.]com
wtar[.]io
zipzone[.]io

IP Addresses:
5[.]183[.]95[.]179
5[.]253[.]43[.]92
38[.]54[.]2[.]119
38[.]54[.]2[.]223
38[.]54[.]2[.]238
45[.]86[.]163[.]182
45[.]86[.]231[.]100
45[.]86[.]231[.]222
45[.]143[.]166[.]125
45[.]155[.]250[.]228
46[.]30[.]188[.]19
46[.]30[.]188[.]161
46[.]30[.]189[.]26
46[.]246[.]96[.]198
51[.]195[.]49[.]222
79[.]110[.]52[.]192
79[.]141[.]164[.]56
85[.]17[.]9[.]18
89[.]150[.]57[.]192
89[.]150[.]57[.]234
128[.]199[.]39[.]196
138[.]199[.]153[.]155
141[.]164[.]37[.]66
146[.]70[.]81[.]33
146[.]70[.]88[.]93
154[.]205[.]146[.]159
158[.]247[.]205[.]35
158[.]247[.]222[.]189
158[.]247[.]254[.]22
162[.]19[.]214[.]208
169[.]239[.]128[.]22
169[.]239[.]128[.]42
169[.]239[.]128[.]46
169[.]239[.]128[.]48
169[.]239[.]128[.]138
169[.]239[.]128[.]160
169[.]239[.]128[.]174
169[.]239[.]128[.]182
169[.]239[.]129[.]57
169[.]239[.]129[.]63
169[.]239[.]129[.]77
169[.]239[.]129[.]100

```
169[.]255[.]58[.]14
169[.]255[.]58[.]18
172[.]233[.]116[.]151
185[.]158[.]248[.]139
185[.]158[.]248[.]146
185[.]167[.]60[.]33
185[.]236[.]202[.]161
185[.]243[.]114[.]170
188[.]166[.]0[.]154
193[.]29[.]56[.]52
193[.]29[.]59[.]176
193[.]168[.]143[.]206
193[.]243[.]147[.]42
195[.]54[.]160[.]224
```

Appendix B: Domain Resolutions

Domain	IP Address	ASN	First Seen	Last Seen
asistentcomercialonline[.]com	169[.]255[.]58[.]14	AS329184	2024-08-15	2025-04-19
barbequebros[.]com	46[.]30[.]188[.]161	AS199959	2024-11-08	2025-04-10
boundbreeze[.]com	188[.]166[.]0[.]154	AS14061	2024-09-20	2025-04-21
branchbreeze[.]com	172[.]233[.]116[.]151	AS63949	2024-11-21	2025-03-29
c3p0solutions[.]com	185[.]167[.]60[.]33	AS46475	2024-08-30	2025-04-18
caddylane[.]com	169[.]255[.]58[.]18	AS329184	2024-04-04	2025-04-02
canylane[.]com	169[.]239[.]128[.]42	AS61138	2025-01-09	2025-04-11
clockpatcher[.]com	85[.]17[.]9[.]18	AS60781	2024-09-16	2025-04-16
colabfile[.]com	141[.]164[.]37[.]66	AS20473	2024-07-19	2025-04-23
craftilly[.]com	128[.]199[.]39[.]196	AS14061	2025-03-05	2025-04-16
dollgoodies[.]com	162[.]19[.]214[.]208	AS16276	2024-03-13	2025-03-08
drivemountain[.]com	169[.]239[.]128[.]22	AS61138	2024-09-04	2025-04-08
eclipsemonitor[.]com	193[.]243[.]147[.]42	AS16276	2024-07-18	2025-04-22
flickerxxx[.]com	169[.]239[.]129[.]57	AS61138	2024-06-12	2025-04-22
gamestuts[.]com	45[.]86[.]163[.]182	AS44066	2024-09-03	2025-04-18
gettravelright[.]com	46[.]30[.]189[.]26	AS44066	2024-09-03	2025-04-08
gilfonts[.]com	38[.]54[.]2[.]223	AS138915	2024-06-27	2025-04-18
gobbledgums[.]com	169[.]239[.]128[.]138	AS61138	2024-11-13	2025-04-18
humansprinter[.]com	158[.]247[.]222[.]189	AS20473	2024-07-18	2025-04-22
infoshoutout[.]com	158[.]247[.]205[.]35	AS20473	2024-07-19	2025-04-22
keep-badinigroups[.]com	5[.]253[.]43[.]92	AS44477	2024-07-01	2025-04-22
lawrdo[.]com	38[.]54[.]2[.]119	AS138915	2024-06-27	2025-04-12
longtester[.]com	193[.]168[.]143[.]206	AS39622	2024-09-16	2025-04-22

mappins[.]io	146[.]70[.]81[.]33	AS9009	2024-04-02	2025-02-20
mdundobeats[.]com	169[.]239[.]129[.]77	AS61138	2024-06-12	2025-04-22
mountinnovate[.]com	79[.]110[.]52[.]192	AS9009	2024-09-27	2025-04-23
mundoautopro[.]com	169[.]239[.]128[.]48	AS61138	2025-02-07	2025-04-1
myprivatedrive[.]net	46[.]30[.]188[.]19	AS199959	2024-07-11	2025-05-02
myread[.]io	185[.]158[.]248[.]146	AS9009	2024-09-24	2025-04-22
mystudyup[.]com	185[.]158[.]248[.]139	AS9009	2024-03-14	2025-03-13
nightskyco[.]com	193[.]29[.]59[.]176	AS48314	2024-09-02	2025-04-17
noticiafamosos[.]com	169[.]239[.]128[.]174	AS61138	2024-06-12	2025-04-19
noticiafresca[.]net	169[.]239[.]128[.]46	AS61138	2025-01-23	2025-03-29
onelifestyle24[.]com	169[.]239[.]128[.]174	AS61138	2024-03-29	2025-03-28
openstreetpro[.]com	45[.]86[.]231[.]222	AS62005	2024-09-18	2025-04-10
pedalmastery[.]com	89[.]150[.]57[.]192	AS59711	2024-07-10	2025-04-23
pinnedplace[.]com	158[.]247[.]254[.]22	AS20473	2024-07-19	2025-04-23
remixspot[.]com	154[.]205[.]146[.]159	AS138915	2024-09-02	2025-04-09
roadsidefoodie[.]com	169[.]239[.]129[.]100	AS61138	2024-08-14	2025-04-11
secneed[.]com	79[.]141[.]164[.]56	AS59711	2024-07-26	2025-04-23
secsafty[.]com	45[.]143[.]166[.]125	AS62005	2024-07-26	2025-04-23
shopstodrop[.]com	185[.]243[.]114[.]170	AS48314	2024-01-18	2025-01-16
speedbrawse[.]com	146[.]70[.]88[.]93	AS9009	2024-07-18	2025-04-23
stableconnect[.]net	51[.]195[.]49[.]222	AS16276	2024-07-05	2025-03-28
starryedge[.]com	169[.]239[.]128[.]160	AS61138	2024-09-04	2025-04-21
statuepops[.]com	89[.]150[.]57[.]234	AS59711	2025-02-11	2025-03-30
steepmatch[.]com	193[.]29[.]56[.]52	AS48314	2025-01-28	2025-05-01
streamable-vid[.]com	195[.]54[.]160[.]224	AS62005	2024-09-20	2025-04-13
strictplace[.]com	5[.]183[.]95[.]179	AS44066	2024-09-13	2025-03-2

svcsync[.]com	169[.]239[.]129[.]63	AS61138	2024-07-10	2025-04-23
themastersphere[.]com	38[.]54[.]2[.]238	AS138915	2024-09-03	2025-04-23
traillites[.]com	138[.]199[.]153[.]155	AS24940	2025-02-01	2025-04-21
trigship[.]com	185[.]236[.]202[.]161	AS9009	2024-01-17	2025-01-15
unibilateral[.]com	169[.]239[.]128[.]182	AS61138	2024-11-13	2025-04-20
updatepoints[.]com	46[.]246[.]96[.]198	AS42708	2024-07-10	2025-04-23
wtar[.]io	45[.]86[.]231[.]100	AS62005	2024-01-31	2025-01-16
zipzone[.]io	45[.]155[.]250[.]228	AS42708	2024-06-27	2025-04-04

Tier 1 domains and associated IP addresses linked to Predator (Source: Recorded Future)

Appendix C: 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 threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering customers to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com