Predator Spyware Resurgence: Insikt Group Exposes New Global Infrastructure

By Insikt Group®

Archived: 2026-04-05 15:58:10 UTC

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, 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).

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, 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 *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**).

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.

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.
