The Predator spyware ecosystem is not dead

By Sekoia TDR, Felix Aimé and Maxime A.

Published: 2024-02-28 · Archived: 2026-04-06 03:17:21 UTC

4 minutes reading

Context

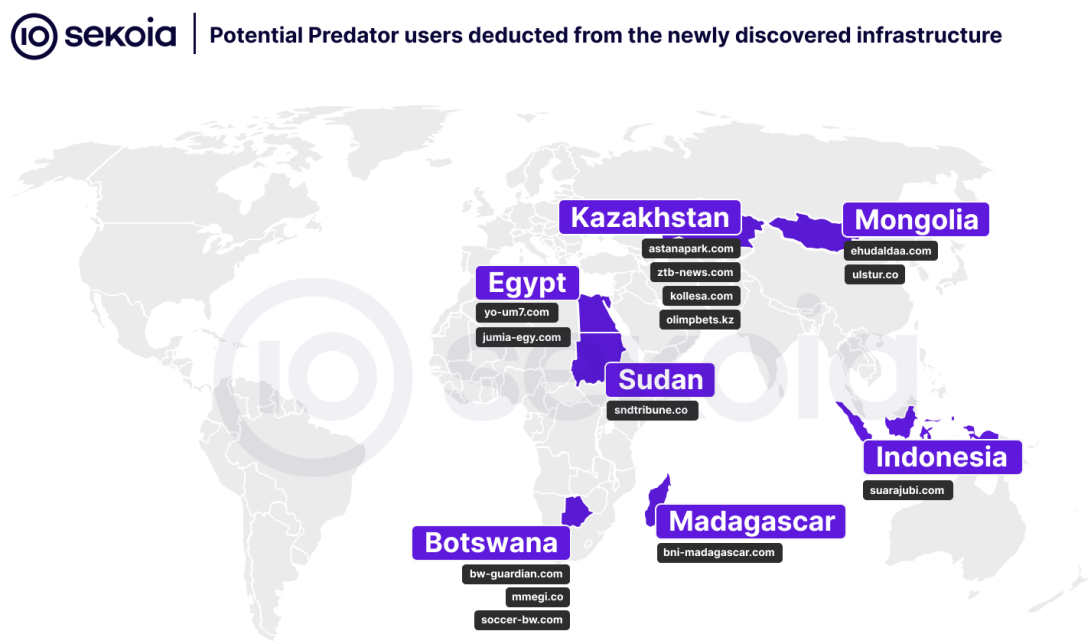
In September and October 2023, several open source publications, part of the *Predator Files project* coordinated by the European Investigative Collaborations, exposed the **use of the Predator spyware** by customers of Intellexa surveillance solutions. The intrusion set related to these customers is tracked under the code-name **Lycantrox** by Sekoia.

Alongside Amnesty International, CitizenLab or MediaPart, Sekoia.io published the blogpost Active Lycantrox infrastructure illumination exposing exploits-related and command-and-control infrastructure clusters employed by Intellexa customers. The publications **forced the shutdown of exposed infrastructure**, hindering the reported use of the spyware against civil society, journalists, politicians or academic targets.

As all *Predator Files* publications exposed users, technical infrastructure and alleged targets, we assumed the spyware use would at least temporarily decrease, or simply end. But no, the Predator ecosystem isn't dead: **we found new infrastructure built after the *Predator Files* publications,** proving Predator is still used nowadays.

As **Sekoia.io officially supported** in February 2024 the **Pall Mall Process** – tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities, we have decided to share related infrastructure with our partners and expose a few domains, with possible related customers once again, in this blogpost.

Alleged customers analysis



Operational security changes for plausible deniability

In a general overview of the newly exposed infrastructure, we noticed a **significant increase in the number of generic malicious domains** which do not give indications on targeted entities and possible customers of Intellexa surveillance solutions.

We assess that some government services that use Intellexa surveillance solutions have taken notice of publications like ours, and **adapted their process** to keep using the solution without giving hints about their targets.

Angola

In our previous paper, we exposed several domains associated with **Angola** entities, some of them were mimicking online media, and others were related to national entities (telecom operators, the national oil company, the national postal service). Such targets made us assess that Angola government services were probably customers of Intellexa surveillance solutions, a hypothesis correlated with other fellow researchers such as Amnesty International.

In the new infrastructure, we found **Portuguese-speaking malicious domains** but **not directly related to Angola entities**. As no other Portuguese-speaking countries were reported using Predator, we assess with medium confidence that Angola services are **still using Predator** as of mid-February 2024 but have increased their operational security, **looking for more plausible deniability**.

Madagascar

In our previous paper, we assessed that Madagascar government services probably purchased and leveraged Predator spyware to conduct political domestic surveillance, especially the month before the 9 November 2023

presidential election.

As other media also pointed out this hypothesis, President Rajoelina acknowledged the use of Predator in an interview to the French media RFI on October 18th 2023. Thus it is **possible** Madagascar Predator users **increased their operational security**, leading to fewer noticeable malicious domains.

A domain still caught our attention, although it is not directly related to Madagascar but to the French newspaper Le Monde (fr-monde[.]com, created on 15 December 2023). This typosquatting can be related to the **French newspaper Le Monde**'s coverage of the use of Intellexa surveillance technologies by Madagascar, whether it is not possible to assess if it was a phishing aimed at Malagasy individuals or Le Monde journalists. However, we associate this domain to Madagascar with medium confidence as it resolved the same IP address (169.239.129[.]76) as bni-madagascar[.]com, another Lycantrox-related domain name weaponized last year.

For other users, business as usual

Indonesia

In our previous investigation, we found malicious domains likely mimicking Jubi TV, a West Papua province opposition media. We assessed it was possible Indonesian services purchased and leveraged Intellexa surveillance solutions to conduct political surveillance, at least on autonomist movements. **The new domains we found confirm our hypothesis**. Among them, kejoranews[.]net likely typosquat Kejora News (the real website is www.kejoranews.com), a media based in the **Riau Islands province.** The second one – suarapapua[.]co – mimics Suara Papua (suarapapua.com), a media also based in **West Papua province,** like previously seen with Jubi TV.

Thus, **no significant operational change** can be observed from the alleged Indonesian use of Predator.

Kazakhstan

For Kazakhstan, it looks like business as usual: a continuation of Predator malicious domains that easily points Kazakhs entities, including medias (vlast-news[.]com), administrative services – cabinet-salyk[.]kz and e-kgd[.]kz – or generics domains with a .kz TLD.

Sekoia.io noticed **no operational change** from the alleged Kazakhstan use of Intellexa surveillance solutions. Astana services **may not be concerned with public exposure**, as Kazakhstan already has a troubled history with cyber surveillance vendors such as NSO, RCS Lab or FinFisher for compromising devices belonging to human right activists, politicians, journalists and opponents.

Egypt

The new infrastructure includes at least 3 domains related to Egypt, mimicking entities related to the media (yo-um7[.]com), fintech (myfawry[.]net) or e-commerce (jumia-egy[.]com) sectors. **Sekoia.io does not notice a significant change** in the plausible deniability of Egypt-related Predator malicious domains.

Newly discovered potential customer countries

Last but not least, we discovered domains related to three countries not included in our previous paper: **Botswana** (mmegi[.]co), **Mongolia** (ulstur[.]co) and **Sudan** (sdntribune[.]co). The last two were reported as using Predator by Amnesty International and other publications related to the *Predator Files*.

Conclusion

Sekoia TDR analysts continue to monitor cyber mercenary groups, such as the Predator infrastructure used by Intellexa customers, contributing to the effort to tackle the proliferation and irresponsible use of commercial cyber intrusion capabilities as promoted by the Pall Mall Process.

If you are an NGO working to protect the civil society against cyber threats, do not hesitate to send us an email to **tdr@sekoia.io** in order to get in touch and share reports and indicators of compromise.

Share

CTI Intellexa Pall Mall Process Predator Predator Files

Share this post:
