Predator Spyware Infrastructure Resurfaces Post-Sanctions – What You Need to Know

By Insikt Group®

Archived: 2026-04-05 16:54:08 UTC

Following exposure and sanctions by the US government, Intellexa's Predator spyware activity appeared to decline. However, recent findings by Insikt Group reveal that Predator's infrastructure is back with modifications to evade detection and anonymize users. This resurgence highlights Predator's ongoing use by customers in countries such as the Democratic Republic of the Congo (DRC) and Angola. While Predator continues to pose significant privacy and security risks, especially to high-profile individuals like politicians and executives, new infrastructure changes make tracking users more difficult. Despite these efforts, defenders can mitigate risks by following cybersecurity best practices, including regular device updates, using lockdown mode, and deploying mobile device management systems. As spyware like Predator evolves, global efforts to regulate and curb its use remain crucial.

After Intellexa, the creators of the infamous Predator spyware, faced sanctions and exposure, a noticeable reduction in Predator activity was observed. However, according to recent analysis by the Insikt Group, Predator is far from disappearing. The spyware infrastructure has resurfaced, posing renewed risks to privacy and security. With its return, operators have implemented new methods to obscure their activities, complicating efforts to trace and attribute their attacks.

The Resurgence of Predator Spyware Infrastructure

In 2024, public reporting and US government sanctions led to a sharp decline in Predator spyware activity. At the time, it appeared that global political efforts aimed at curbing spyware abuse were making significant progress. However, Insikt Group's recent findings point to a re-emergence of Predator's infrastructure. New infrastructure tied to Predator was detected in multiple countries, including the Democratic Republic of the Congo (DRC) and Angola.

This sophisticated spyware, primarily used by government actors, allows operators to infiltrate devices, gaining access to sensitive data like messages and contacts and even activating cameras and microphones without the user's knowledge.

Changes in Infrastructure and Evasion Tactics

Predator's operators have significantly enhanced their infrastructure, adding layers of complexity to evade detection. The new infrastructure includes an additional tier in its multi-tiered delivery system, which anonymizes

customer operations, making it even harder to identify which countries are using the spyware. This change makes it more difficult for researchers and cybersecurity defenders to track the spread of Predator.

Despite these changes, the mode of operation remains largely the same. The spyware likely continues to use both “one-click” and “zero-click” attack vectors, exploiting browser vulnerabilities and network access to install itself on targeted devices. Even though there are no reports of fully remote zero-click attacks, like those associated with Pegasus, Predator remains a dangerous tool in the hands of those targeting high-profile individuals.

High-Profile Targets Remain at Risk

One of the most concerning aspects of Predator’s return is its likely continued targeting of high-profile individuals. Politicians, executives, journalists, and activists are at the highest risk due to the intelligence value they hold for governments or other malicious actors. The costly licensing of Predator further suggests that operators reserve its use for strategic, high-value targets.

This widespread use of mercenary spyware, particularly against political opposition, has sparked concern in regions like the European Union. Investigations in Greece and Poland have already revealed how spyware has been used against opposition figures and journalists, raising serious questions about the legality and ethics of such surveillance.

Best Practices for Defense

Given Predator's renewed presence and the sophistication of its infrastructure, individuals and organizations must stay vigilant. Insikt Group has outlined several defensive measures that can help mitigate the risk of Predator spyware infiltration:

1. **Regular Software Updates –** Keeping devices up to date with the latest security patches is crucial for reducing vulnerabilities that spyware like Predator exploits.
2. **Device Reboots –** Periodically rebooting devices can disrupt spyware operations, though it may not completely eliminate advanced spyware.
3. **Lockdown Mode –** Activating lockdown mode on devices can help block unauthorized access and exploitation attempts.
4. **Mobile Device Management (MDM) –** Implementing MDM systems allows organizations to manage and secure employee devices, ensuring they adhere to security protocols.
5. **Security Awareness Training –** Educating employees about spearphishing and other social engineering tactics can reduce the likelihood of falling victim to spyware attacks.

These measures are particularly important for individuals in sensitive roles, such as those working in government, civil society, or corporate leadership positions.

The Future of Spyware and Global Regulations

Despite efforts to curb the use of spyware, the market for mercenary spyware is expected to grow. As demand for surveillance tools continues, more companies will likely emerge, developing new products and finding ways to bypass security defenses. The profitability of spyware and the competition within the industry make it likely that we will see even more sophisticated tools in the future.

In response to these threats, global efforts to regulate spyware continue. Investigations like those underway in the European Union may lead to stricter regulations on spyware sales and use. However, until significant international action is taken, Predator and similar tools will remain a persistent threat.

Conclusion

The re-emergence of Predator spyware is a stark reminder of the growing dangers posed by mercenary spyware. While initial sanctions and public exposure seemed to have diminished its presence, recent developments show that Predator is still very much active. Its infrastructure has evolved, making it harder to track and identify users, but with the right cybersecurity practices in place, individuals and organizations can reduce their risk of becoming targets.

As the spyware market continues to expand, it is essential for governments and cybersecurity professionals to stay ahead of these threats. Public reporting, ongoing research, and stronger regulations are critical in minimizing the damage caused by tools like Predator.

To read the entire analysis, click here to download the report as a PDF.

Appendix A — Indicators of Compromise

Appendix B — Mitre ATT&CK Techniques
