CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

September 5, 2024

Predator Spyware Infrastructure Returns Following Exposure and Sanctions

Although Predator spyware was believed to be largely inactive due to major public exposures and US government sanctions, Insikt Group has identified new infrastructure and domains likely involved in the staging and exploitation processes.

The latest evolution of Predator infrastructure includes an additional tier in its delivery infrastructure to improve customer anonymization and enhanced operational security in its server configurations and associated domains.

Insikt Group has identified at least four Predator clusters, including one likely linked to the Democratic Republic of the Congo, which was not covered in our earlier 2024 report.

Note: The analysis cut-off date for this report was August 25, 2024

Executive Summary

Following major public exposures and United States (US) government sanctions against Intellexa, the creators of the prominent mobile spyware Predator, Insikt Group and third-party researchers observed a significant decrease in Predator activity. This apparent downturn in Predator spyware usage led to questions about the extent to which the aforementioned exposures and sanctions, coupled with broader global political initiatives against spyware proliferation, had resulted in a longer-term impact on Intellexa's operations. However, since this period of decreased activity, Insikt Group has identified a swath of new Predator infrastructure likely used during the spyware staging and exploitation process. This infrastructure is likely linked to Predator customers located in multiple countries Insikt research has previously highlighted. We have also identified a newly observed customer in the Democratic Republic of the Congo (DRC) that is likely currently using Predator. Although Predator spyware operators have changed significant aspects of their infrastructure setup, including changes that make country-specific attribution more challenging, they have largely retained their mode of operation.

Deploying spyware like Predator beyond criminal and counterterrorism efforts poses major risks to the privacy, legal protections, and physical safety of both targeted individuals and other related entities. Although most documented abuses involve civil society or political activists, organizations and individuals in regions with a history of spyware abuse should remain cautious, regardless of their industry. Due to Predator's costly licensing model, operators reserve its use for high-profile strategic targets. Politicians, executives, and other persons in sensitive roles are at increased risk of targeting due to their intelligence value. The widespread, likely unlawful use of spyware against the political opposition is currently being addressed in various European Union (EU) countries, including Poland and Greece.

In the short term, as detailed in our previous report on Predator spyware, defenders should follow Insikt Group's suggested best practices. These include ensuring personal and corporate devices are not linked, updating phones regularly, encouraging periodic device reboots (though this may not always eliminate Predator spyware), using lockdown mode, and implementing a mobile device management (MDM) system. Additionally, investing in security awareness training for employees and promoting a culture of minimal data exposure is crucial to reducing the risk of successful spearphishing and limiting the amount of data stolen in the event of a breach.

In the long term, we expect continued growth in the mercenary spyware market, with new companies and products emerging. We also anticipate the identification of new victims beyond civil society. Recent investigations by the Polish and Greek governments into spyware abuse could potentially lead to similar investigations in other countries. Increased innovation in this field is likely due to ongoing demand, company profitability, competition, and improved IT security among targets. Moreover, defensive measures such as continuous public reporting and efforts to eliminate entire classes of security vulnerabilities may make certain targets—like cloud backups accessed via stolen credentials—and alternative spyware deployment methods beyond spearphishing more attractive to spyware operators.

Key Findings

- Insikt Group has identified new Predator spyware infrastructure and domains likely used during the staging and exploitation process. This new infrastructure was discovered through a combination of network artifacts, Recorded Future Network Intelligence, and other indicators.
- In the latest evolution of Predator infrastructure, the operators have added an additional tier to their multi-tiered delivery system to enhance customer anonymization. We also observed enhanced operational security in the delivery server configurations and associated domains.
- Insikt Group identified at least four Predator clusters. One of the clusters is likely connected to the Democratic Republic of the Congo (DRC), which was not covered in our initial Predator report in March 2024.

Background

Predator Spyware

Predator, a sophisticated mercenary spyware for Android and iPhone devices, has been in use since at least 2019. Originally developed by Cytrox and now managed by the Intellexa alliance, it is highly invasive and designed for versatility. Predator leaves minimal traces on target devices, making independent audits of potential abuses challenging. Once installed, it provides unrestricted access to a device's microphone, camera, and all data, including contacts, messages, photos, and videos, without the user's knowledge. Its Python-based modules allow for the addition of new functionalities without repeated exploitation.

According to the leaked "Predator Files" analyzed by Amnesty International, Predator infections are managed via a web-based "Cyber Operation Platform" that allows operators to target specific phones. The Predator system includes the spyware agent, exploits, and attack vectors, with exploits and payloads distributed from an "installation server" and devices connecting to a command-and-control (C2) network. Both the installation and C2 servers must be publicly accessible, while anonymization networks are used to make tracking the operators difficult.

Predator can use "one-click" and "zero-click" attack vectors. "One-click" attacks involve social engineering messages with malicious URLs, which, if clicked, exploit browser vulnerabilities to install the spyware. "Zero-click" attacks, as described in the Predator Files, do not require user interaction and target devices that have privileged network access or are in close proximity using various network injection methods. Unlike NSO Group's Pegasus, no fully remote "zero-click" attacks similar to those involving messaging apps have been reported for Predator.

Mercenary Spyware and Abuse Instances

The mercenary spyware market has expanded, with companies developing and marketing spyware products and services. Although these tools are typically subject to export restrictions and are officially intended for government use to combat terrorism, investigate crimes, and enhance national security, ethical and legal concerns have arisen due to documented abuses. This has drawn public attention to their use. Between 2021 and 2023, numerous instances of attempted and successful Predator infections have been documented affecting individuals in various sectors and countries, including Greece, Egypt, and Vietnam. However, these cases likely represent only a small fraction of the total, given the widespread use of mercenary spyware like Predator, the difficulties in detecting such threats, and the limited forensic support available for investigating potential spyware use.

Factors Behind Recent Reduced Activity

Insikt Group and other researchers observed a significant reduction in Predator activity in the immediate aftermath of Insikt Group's reporting in March 2024 and the aforementioned US government sanctions. This decline is likely due to three main factors: First, there has been a notable increase in public reporting over the past year on Predator infrastructure, techniques, and corporate structures. This likely led to increased costs for both Intellexa and Predator customers and may have led some customers to reconsider their association with the vendor due to heightened public attention and concerns about being linked to human rights abuses. Second, unprecedented sanctions and political actions to curb spyware proliferation—including the US adding Intellexa to its entity list, an EU resolution, a US visa ban on Intellexa affiliates, and the initiation of the Pall Mall Process—are believed to have heavily impacted Intellexa's operations. Finally, from a broader perspective beyond just Predator, it is believed that obtaining effective exploit chains, especially for iPhones, has become more difficult and costly. This is due to advancements in software and hardware security, which have made it more difficult to find exploitable vulnerabilities

Infrastructure Analysis

Identification of New Infrastructure Following Public Reporting

Detection of Delivery Servers

Insikt Group identified a swath of new infrastructure likely being used during Predator spyware's delivery and exploitation process. This infrastructure was detected through a combination of distinctive domain registration patterns, server configurations tied to Predator delivery servers, and Recorded Future Network Intelligence data.

Timeline of Infrastructure Activity

Following Sekoia's public report on October 2, 2023, the number of active Predator delivery servers dropped sharply, indicating a swift response by the operators (see **Figure 1**). Despite this, some delivery servers from "Iteration 1" remained active for a considerable time after the report. From mid-October on, Insikt Group observed and reported to customers the reconstruction of the delivery infrastructure, referred to as "Iteration 2" hereafter. The creation of delivery servers accelerated in the latter half of November 2023 and appears to have stabilized at the beginning of January 2024.

Immediately following Insikt Group's public report on this infrastructure in March 2024, the infrastructure was largely dismantled. Despite the assumption that Predator activity had significantly decreased, Insikt Group identified new clusters of activity, now tracked as "Iteration 3", that emerged during this timeframe: domain registration activity associated with "Iteration 3" began in early January 2024, prior to Insikt Group's public report, and new infrastructure and domains were gradually added over the subsequent months, gaining momentum between the beginning of June and mid-July 2024 with an increase of more than 100% between June 1, 2024, and August 1, 2024. Our assessment indicates that a significant part of this new infrastructure is associated with Predator customer(s) in Angola.

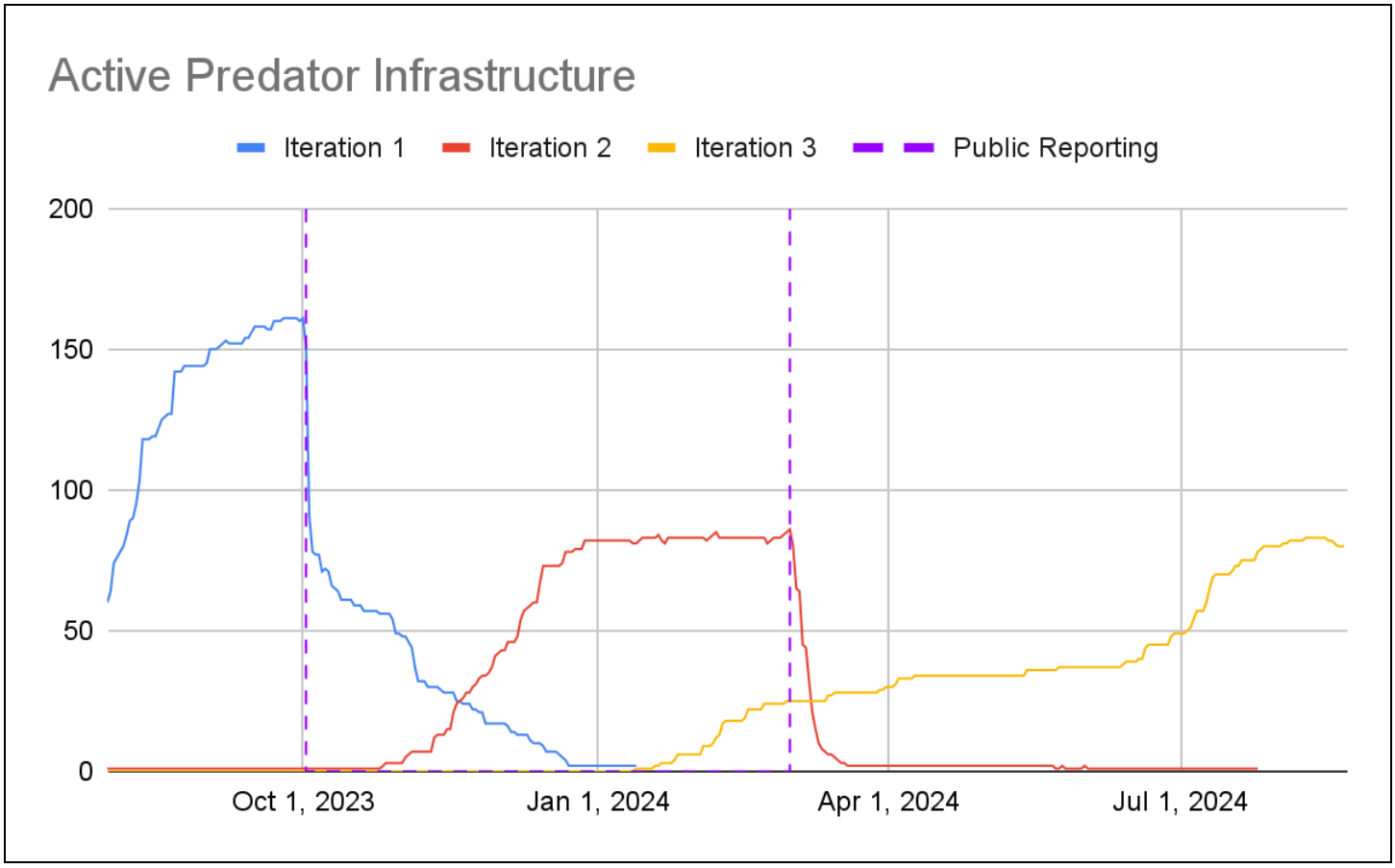

Figure 1: *Active Predator infrastructure before and after public reporting (Source: Recorded Future)*

Network Intelligence

Updated Tiered Delivery Network Architecture

In both "Iteration 1" and "Iteration 2", Insikt Group identified Predator customers using a multi-tiered infrastructure network. This network also mirrors the high-level architecture described in the October 2023 Amnesty International report.

Initially, we observed the deployment of downstream delivery servers akin to those identified in previous research (1, 2, 3). These servers are probably employed for device exploitation and gaining initial access. Typically, they host domains that spoof specific entities of interest to the target, facilitating social engineering attacks.

Through Recorded Future Network Intelligence, we observed that these delivery servers frequently communicated with a consistent upstream virtual private server (VPS) IP address via Transmission Control Protocol (TCP) port 10514. These upstream servers are likely used as hop points for anonymization, thereby minimizing the chances of linking the delivery servers to specific Predator customers.

We also observed consistent communication over TCP port 10514 between these upstream servers and third-tier servers, primarily consisting of leased servers within Autonomous System Numbers (ASNs) previously linked to Predator operations. These third-tier servers then relay traffic to suspected Predator customer-controlled static in-country ISP IP addresses (see **Figure 2**). This represents a significant departure from the previously identified "Iteration 1" and "Iteration 2" activities, which used only a single hop between the delivery servers and the suspected Predator customer-controlled servers. The change, which is marked in blue in **Figure 2**, likely aims to make it more challenging to identify countries suspected of using Predator.

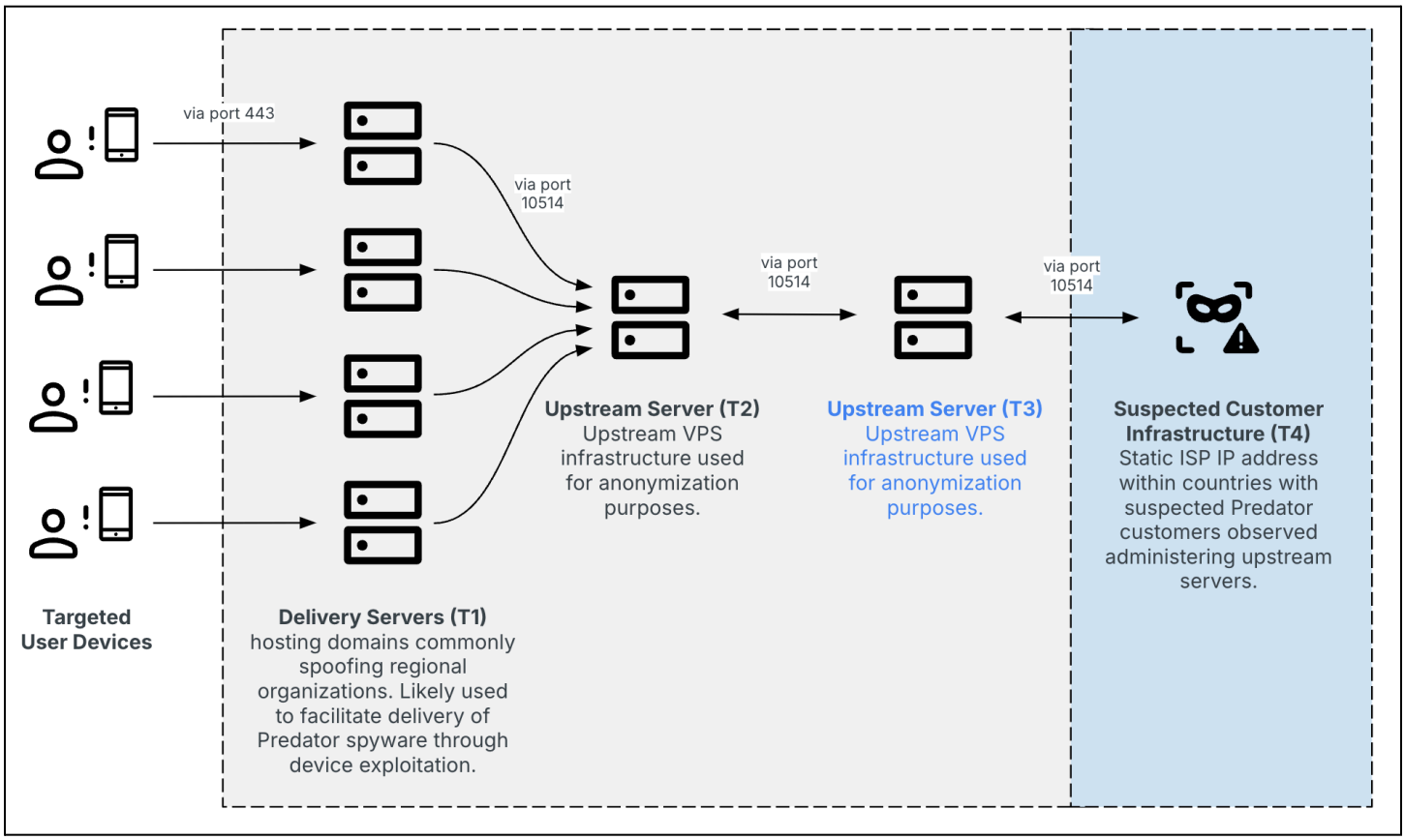

Figure 2: *Multi-tiered Predator infrastructure with additional tier (Source: Recorded Future)*

Identification of Active Clusters

Insikt Group has identified various clusters to date, which are ultimately linked to Predator use within specific countries (see **Figure 3**). Cluster 1 is active and highly likely linked to Angola. Cluster 2 also appears active and is likely linked to the Democratic Republic of the Congo, a country we did not report on in our first report on Predator spyware in March 2024. Cluster 3 also appears active and cannot be conclusively linked to any specific country, though there are potential connections to both Madagascar and the UAE. It is also possible that this cluster represents two distinct clusters. Cluster 4 seems inactive and is likely linked to Saudi Arabia. Alongside these clusters, there are several servers we suspect are closely tied to Predator operations, though we are currently unable to associate them with any specific cluster or country.

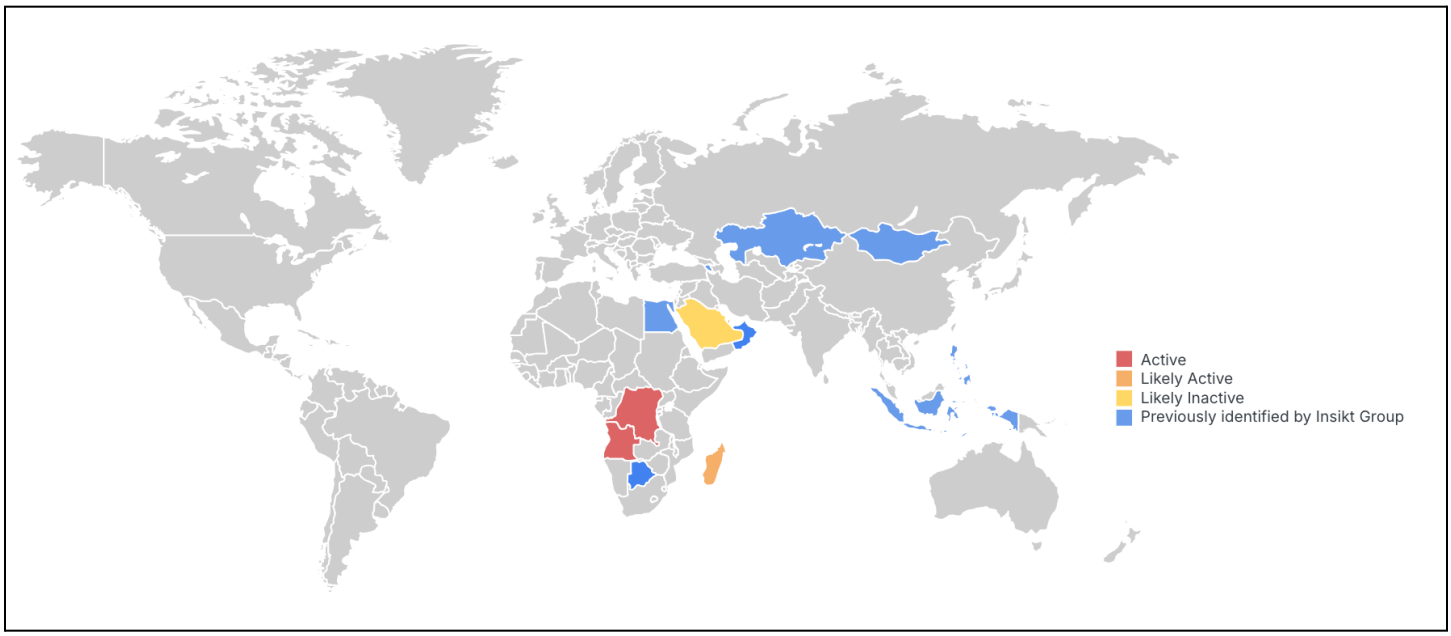

Figure 3: *Countries with suspected Predator customers (Source: Recorded Future)*

Angola

Cluster 1 is highly likely associated with Angola for several reasons. Many of the identified domains were in Portuguese, which aligns with historical delivery domains previously attributed to Angola-based Predator customer(s). Additionally, some servers in this cluster have hosted domains previously linked to Predator activity in Angola and have been seen in communication chains that eventually connected to a static ISP IP address in Angola, which was identified as customer infrastructure. Moreover, we observed suspected Angolan victims communicating with servers in this cluster.

Democratic Republic of the Congo

Cluster 2 is highly likely associated with the Democratic Republic of the Congo. The assessment is based on the observation that some of the domain names appeared to be tailored for specific customer countries and were found in communication chains that ultimately linked to a static ISP IP address in the Democratic Republic of the Congo.

Amnesty International reported that products from the "Intellexa Alliance" have been sold to client(s) in the Democratic Republic of the Congo. Research by Citizen Lab also identified domain naming patterns indicative of potential use in the Democratic Republic of the Congo. Additionally, the country has a history of employing surveillance technologies. For instance, in 2019, an investigation by the Israeli television program Uvda revealed that Israeli intelligence firm Black Cube had supported the Congolese government with extensive surveillance, including wiretapping political opposition and activists since 2015, especially during election periods. Furthermore, the Media Policy and Democracy Project (MPDP) in South Africa suggested that the government likely acquired surveillance technology from Israel's

NSO Group and Germany's PKI Electronic Intelligence, based on interviews with members of state security agencies and telecom companies.

Armed conflict continues to plague the DRC — as noted by Amnesty International, in 2023 "dozens of armed groups remained active, mainly in the eastern provinces of Ituri, Nord-Kivu, and Sud-Kivu". These conflicts include clashes between Congolese authorities and the Rwandan-backed March 23 Movement (M23) rebels, among others. Notably, at least one of the domains (*nyirangongovrai[.]com*) associated with the cluster linked to the DRC has a clear connection to the eastern provinces (see **Table 1**). Mount Nyiragongo, a volcano located within Virunga National Park, is situated in a region heavily affected by armed conflict.

Domain	IP Address	First Seen
happytotstoys[.]com	185.243.113[.]169	2024-02-08
toysfourtots[.]com	45.86.163[.]178	2024-02-08
holidaypriceguide[.]com	185.243.113[.]169	2024-02-21
nyirangongovrai[.]com	98.142.253[.]18	2024-04-03
masoloyakati[.]com	185.235.137[.]6	2024-04-03
lesautreseux[.]com	193.29.59[.]164	2024-04-03
noisyball[.]com	193.29.56[.]252	2024-07-19
yokananu[.]net	185.123.102[.]40	2024-07-19

Table 1: *Selection of Predator delivery domains likely linked to the Democratic Republic of the Congo (Source: Recorded Future)*

Suspected Madagascar or UAE

Cluster 3 is likely linked either to Madagascar or the UAE, and it's possible that it represents two distinct clusters. On one hand, domains previously associated with Madagascar have been hosted on servers within Cluster 3, suggesting a connection to Madagascar. However, we have observed multiple cases in which delivery servers used by one Predator customer were later used for other customers, complicating this association. For example, the IP address *169.239.129[.]76*, which was associated with a previous Predator iteration, initially hosted a domain related to Madagascar. Later, it began hosting a domain linked to Angola and was observed communicating with an Angola-based upstream server.

On the other hand, we detected two suspected UAE-based victim IP addresses communicating with a Predator server within Cluster 3. This server also concurrently hosted a domain linked to another server within Cluster 3 based on a shared registrant email address. The second associated server has been observed communicating with the upstream server hosting Madagascar-related domains.

Several possibilities should be considered. One is that the email address was used for registering domains for both Madagascar- and UAE-based customers, which aligns with the suspicion that Intellexa directly handles customer infrastructure, as noted in our previous report. Another is that a Predator customer in Madagascar targeted UAE-based victims. Lastly, it's possible that servers initially tied to Madagascar-related domains are now used by a different customer, indicating that Cluster 3 might be linked to the UAE rather than Madagascar.

Saudi Arabia

Cluster 4 appears to be associated with Saudi Arabia. Given the domain registration date and the lack of additional infrastructure, we assess that this cluster is currently inactive. Additionally, the higher-tier infrastructure linked to this cluster was noted in our previous reports earlier this year, suggesting that it is likely leftover infrastructure.

Outlook

Insikt Group has found evidence indicating that Predator continues to be used in several countries despite extensive media coverage and sanctions against Intellexa and related entities. These actions have likely resulted in substantial costs for both the clients and Intellexa, leading to a widespread belief that its operations had largely subsided. Our findings show that while Predator operators did modify certain aspects of their infrastructure in response to public reporting, including elements of their higher-tier infrastructure and tactics for detection evasion, they maintain their operations with minimal changes and often even reuse previously identified infrastructure, in line with previous observations. The ongoing proliferation of Predator and other spyware products, along with hack-for-hire services outside of serious crime and counterterrorism contexts, poses a significant threat to various organizations and individuals.

Appendix A — Indicators of Compromise

Domains:
happytotstoys[.]com
holidaypriceguide[.]com
lesautreseux[.]com
masoloyakati[.]com
noisyball[.]com
nyirangongovrai[.]com
toysfourtots[.]com
yokananu[.]net

IP Addresses:
169.239.129[.]76
185.123.102[.]40
185.235.137[.]6
185.243.113[.]169
185.243.113[.]169
193.29.56[.]252
193.29.59[.]164
45.86.163[.]178
98.142.253[.]18

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

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 clients, 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 clients 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