CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

March 1, 2024

Predator Spyware Operators Rebuild Multi-Tier Infrastructure to Target Mobile Devices

Note: The analysis cut-off date for this report was January 15, 2024. We also note subsequent February 2024 reporting from Sekoia which corroborates our findings.

Executive Summary

Following a string of major public disclosures, Insikt Group has identified new infrastructure associated with operators of the mercenary mobile spyware Predator. In particular, we identified evidence of the likely continued use of Predator within at least eleven countries, specifically Angola, Armenia, Botswana, Egypt, Indonesia, Kazakhstan, Mongolia, Oman, the Philippines, Saudi Arabia, and Trinidad and Tobago. Before this, no Predator customers within Botswana and the Philippines had been identified. Although ostensibly sold for counterterrorism and law enforcement applications, there has been a well-documented trend of Predator usage targeting civil society, including journalists, politicians, and activists (1, 2, 3, 4). At this time, we have not identified specific victims or targets of this latest Predator activity.

Domestic use of mercenary spyware such as Predator outside of serious crime and counterterrorism law enforcement use cases continues to pose privacy, legal, or physical safety risks for end targets, their employers, and the entities conducting this activity. Although most abuse cases are associated with civil society targeting, other organizations and individuals in regions known for spyware abuse or who see themselves as potential targets should be mindful of the risk, regardless of industry or location. Due to the high deployment costs with charges per infection, high-profile individuals who are expected to have significant intelligence value, including executives, are more likely to be targeted. The continued and pervasive use of mercenary spyware has recently been addressed by the European Union (EU) through a resolution aimed at curbing its abuse among member states.

In the short term, defenders should adopt security best practices, such as ensuring regular phone updates, promoting regular device reboots (while acknowledging that this might not always remove Predator spyware), advocating for the use of lockdown mode, implementing a Mobile Device Management (MDM) system, and enforcing the separation of personal and corporate devices. These practices should be paired with investments in security awareness training for employees and fostering a culture of minimal data exposure. For a longer-term solution, organizations should invest in risk assessments to develop more nuanced and dynamic security policies.

As the market for mercenary spyware expands with new companies and products, the risk of being targeted by them or the related hack-for-hire industry is no longer limited to civil society groups; instead, this risk threatens anyone of interest to entities with access to these tools or tools with comparable capabilities. At the same time, continued profitability, growing competition, and heightened IT security will drive innovation, leading to stealthier infection chains (for example, enabling persistence despite factory resets), alternative targets such as cloud backups, a more professionalized spyware ecosystem, and more comprehensive portfolios. Therefore, effective mitigations require monitoring the ecosystem closely, assessing associated risks, and policymakers implementing more effective regulations.

Key Findings

- Insikt Group identified a new multi-tiered Predator delivery infrastructure network consisting of delivery servers, upstream servers, and infrastructure highly likely associated with Predator customers. Our findings illustrate the spyware operators' initial response to public reporting in September 2023, as well as their continued efforts thereafter with minimal changes to their mode of operation.
- Further evidence obtained through domain analysis and Recorded Future Network Intelligence data identified likely Predator customers within at least eleven countries, specifically Angola, Armenia, Botswana, Egypt, Indonesia, Kazakhstan, Mongolia, Oman, the Philippines, Saudi Arabia, and Trinidad and Tobago. Prior to this, no customers within Botswana and the Philippines had been identified.
- While Predator stands out as one of the premier providers of mercenary spyware, alongside NSO Group's Pegasus, the tactics, techniques, and procedures (TTPs) it uses during its delivery process have remained consistent over time, likely indicating their ongoing success.

Background

Predator Spyware

Predator, a sophisticated mercenary spyware designed for use on both Android and iPhone devices, has existed since at least 2019. It was initially developed by Cytrox and is currently managed by the Intellexa alliance[1]. This highly invasive spyware was crafted for versatility, likely leaving very limited traces on the target device and making independent audits of potential abuses highly complex. Upon infiltration, Predator gains unfettered access to a device's microphone, camera, and all stored or transmitted data, including contacts, messages, photos, and videos — all without the user's knowledge. Its design incorporates Python-based modules, facilitating the introduction of new functionalities without the need for repeated exploitation.

Based on leaked documents referred to as the "Predator Files" and analyzed by Amnesty International, Predator infections are managed through a web-based system referred to as the "Cyber Operation Platform", which allows the spyware operator to target specific phones. The complete Predator system comprises various elements, such as the spyware agent, exploits, and attack vectors. Exploits and payloads are distributed from an "installation server", and, upon infection, the device connects to a command-and-control (C2) network. Both the "installation server" and C2 server must be publicly accessible on the internet for connections from targeted devices. Operators can issue commands, such as to retrieve specific files or activate the device's microphone. An anonymization network obscures the operator's location and identity, making attribution of attacks more challenging.

[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 the press release. The current status of this alliance remains unclear.

Both "1-click" and "zero-click" attack vectors can be used to target and infect specific devices. Previously documented attacks associated with Predator involved social engineering messages with malicious URLs, known as "1-click" attacks (1, 2, 3). These attacks depend on building trust with the target and customizing the attack to lure them into opening the link. If the link is clicked, and the targeted phone operates on a supported browser and operating system version, the exploit chain is triggered. This chain compromises the web browser before attempting to escalate privileges and install the spyware agent on the device. The power of "1-click" attacks lies in their ability to reach targets irrespective of their geographical location.

Furthermore, the "Predator Files" outline diverse techniques provided by the Intellexa alliance for installing the spyware through "zero-click" attacks, eliminating the need for user action like clicking on a link. These non-remote "tactical attacks" allow spyware operators to target devices with privileged network access or in close physical proximity, utilizing various network injection methods and attacks against mobile phone basebands. To date, there have been no reports of fully remote "zero-click" attacks similar to those seen in NSO Group's Pegasus (for example, FORCEDENTRY or BLASTPASS) infections used by Predator. These attacks usually entail remotely exploiting vulnerabilities in popular messaging apps such as iMessage or WhatsApp.

Predator Abuse Instances and Mercenary Spyware Market

The mercenary spyware market has increased, with companies developing and marketing spyware products and services. While often under export restrictions and officially designed for government purposes to prevent terrorism, investigate crime, and enhance national security, ethical and legal concerns have emerged in recent years due to instances of abuse, drawing public attention to the deployment of these surveillance tools. Between 2021 and 2023, diverse instances of attempted and successful Predator infections have been documented, affecting individuals across various sectors and countries, including Greece, Egypt, and Vietnam. Notable examples between 2021 and 2023 include:

- In **December 2021**, Citizen Lab reported on two Egyptians, the exiled politician Ayman Nour and an anonymous host of a popular news program, who had been successfully infected with Predator after clicking on links sent via WhatsApp.
- In **April 2022**, Inside Story reported that Thanasis Koukakis, a journalist at News and contributor to various news outlets such as CNN, had been successfully infected with Predator.
- In **July 2022**, Documento revealed that Nikos Androulakis, the leader of an opposition party in Greece and a sitting Member of the European Parliament, had been unsuccessfully targeted by Predator in 2021 and wiretapped by the Greek National Intelligence Service (NIS).
- In **March 202**, Artemis Seaford, a Meta executive with dual US-Greek citizenship, was reportedly targeted with Predator and allegedly wiretapped by the NIS.
- In **September 2023**, Citizen Lab revealed that Ahmed Eltantawy, a former Egyptian Member of Parliament, had been targeted multiple times with Predator between 2021 and 2023. The attacks used various infection vectors, including links in SMS and WhatsApp messages, as well as network injections.

- In **October 2023**, Amnesty International revealed a surveillance operation by a Predator customer linked to Vietnam targeting at least 50 social media accounts belonging to 27 individuals and 23 institutions between February and June 2023. The infection links were sent from a social media account to multiple targets, including a Berlin-based independent news website, political figures in the European Parliament, the European Commission, academic researchers, various think tanks, and attempted targets like United Nations officials, the President of Taiwan, US senators and representatives, and other diplomatic authorities.

While the described instances hold significance on their own, they are likely only a representative fraction, considering the widespread use of mercenary spyware like Predator, the challenges associated with detection, and the limited support available for victims.

Threat Analysis

Identification of Delivery Servers

Initial Detection of Delivery Servers

Leveraging artifacts reported by Citizen Lab in September 2023, Insikt Group identified distinctive server configurations connected to Predator delivery servers. Coupled with information on suspected customer locations and delivery domain naming conventions, we identified and reported on additional delivery servers and domains, which were later confirmed by a public report from Sekoia. These detections are referred to as “Iteration 1” in this report.

Timeline of Delivery Server Activity

Immediately following Sekoia's public report on October 2, 2023, the number of active Predator delivery servers plummeted, indicating that the operators quickly responded to the report (see **Figure 1**). Despite the activity, some delivery servers from “Iteration 1” continued to be active for a significant amount of time following the report. Starting in mid-October, Insikt Group noted the reconstruction of the delivery infrastructure, referred to as “Iteration 2” hereafter, and reported on it internally. Delivery server creation gained momentum in the latter half of November and seems to have reached a plateau at the beginning of January 2024.

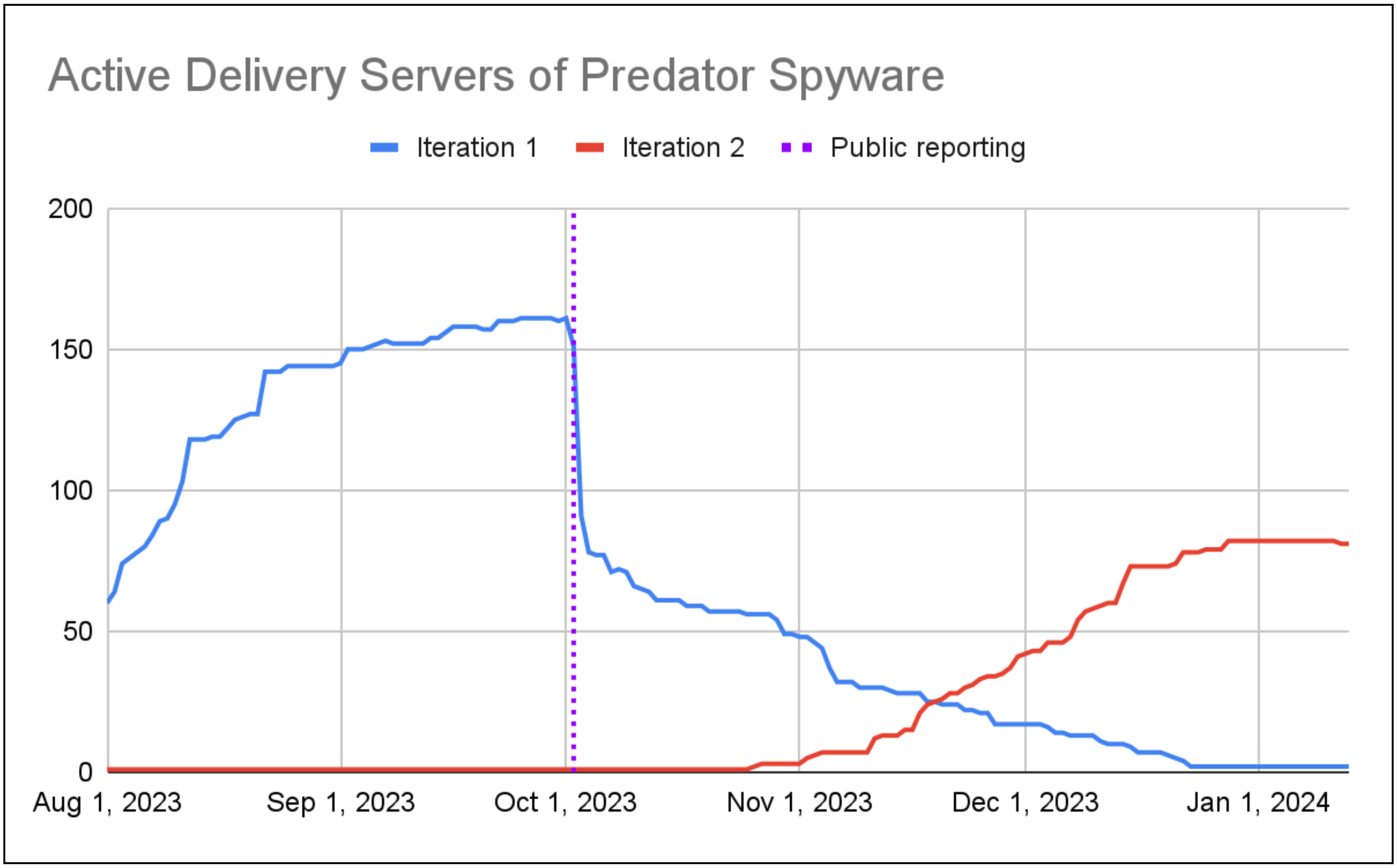

Figure 1: *Active delivery servers of Predator spyware during "Iteration 1" and "Iteration 2" (Source: Recorded Future)*

While it is possible that the domains and delivery servers observed during "Iteration 1" only appeared active due to improper infrastructure takedown, the possibility that they were still being actively used for campaigns cannot be ruled out.

Validation Strategies for Delivery Servers

In addition to distinctive server configurations and domain naming conventions, various validation strategies were used to enhance confidence that the suspected delivery servers from "Iteration 2" were indeed part of the Predator delivery server network.

- As noted by Sekoia, the nginx instances on Predator delivery servers are set up to complete a TLS handshake only when a valid domain name is provided; otherwise, it responds with an `SSL_ERROR_UNRECOGNIZED_NAME_ALERT`, leading to a dropped connection.
- In addition, leveraging Recorded Future Network Intelligence, Insikt Group observed regular communication between many suspected delivery servers and the identified upstream servers.
- Finally, Insikt Group identified an additional approach for validating Predator delivery domains, relying on network-related artifacts that have consistently appeared across both iterations.

Grouping of Delivery Domains by Themes and Countries

Domain Naming Theme Analysis

Predator delivery domains have consistently exhibited similar naming patterns. Though not always mutually exclusive (for example, *newsworldsports[.]co*) and occasionally unclear (for example, *stlk[.]info*), these patterns can roughly be grouped into eight themes and match with prior reporting (see **Table 1**).

Theme	Example	Note
News	mundodenoticias[.]online	Spoofing a generic Portuguese or Spanish news domain
Sports	soccer-bw[.]com	Spoofing a generic sports website with a possible connection to Botswana
Weather	weather-live[.]com	Spoofing a generic live weather forecast website
Generic / Technical	get-location[.]com	Spoofing a generic, technical-sounding domain
Commercial	kollesa[.]com	Likely spoofing *kolesa[.]kz*, a Kazakh auto sales platform
Notification	notify-service[.]biz	Spoofing a generic domain, suggesting a use for notifications
Specific entity	spacsaver[.]info	Likely spoofing *specsavers[.]com*, a British retail company
Erotics	sexychats[.]nl	Likely spoofing a generic erotic chat platform domain

Table 1: *Predator delivery domain naming themes with examples (Source: Recorded Future)*

Accounting for nearly 25% of all delivery domains in both iterations, typosquatting of specific or generic news domains appears to have a significant role in Predator delivery and has been noted by other researchers (see **Figure 2**). Though information about Predator infection chains is limited, this knowledge offers insight into potential lure types they employ.

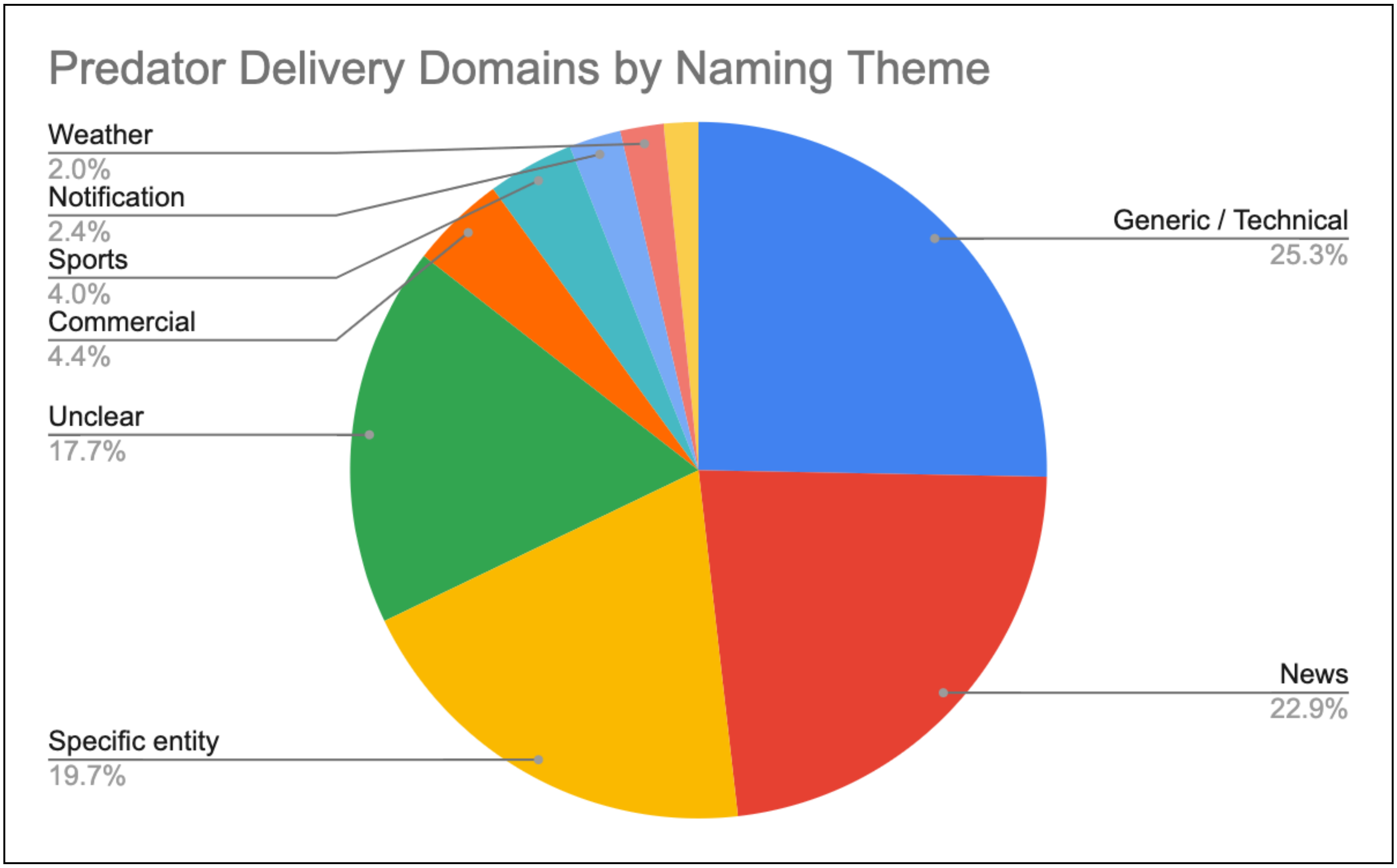

Figure 2: *Predator delivery domains by naming theme (Source: Recorded Future)*

Identification of Suspected Predator Usage Within Specific Countries

Numerous domains also reveal distinct ties to specific countries or regions, many of which are unknown or suspected locations of Predator customers (see **Figure 3**). This information enhances our understanding of Predator's potential customer base and allows for a comparative assessment of infection prevalence in specific countries.

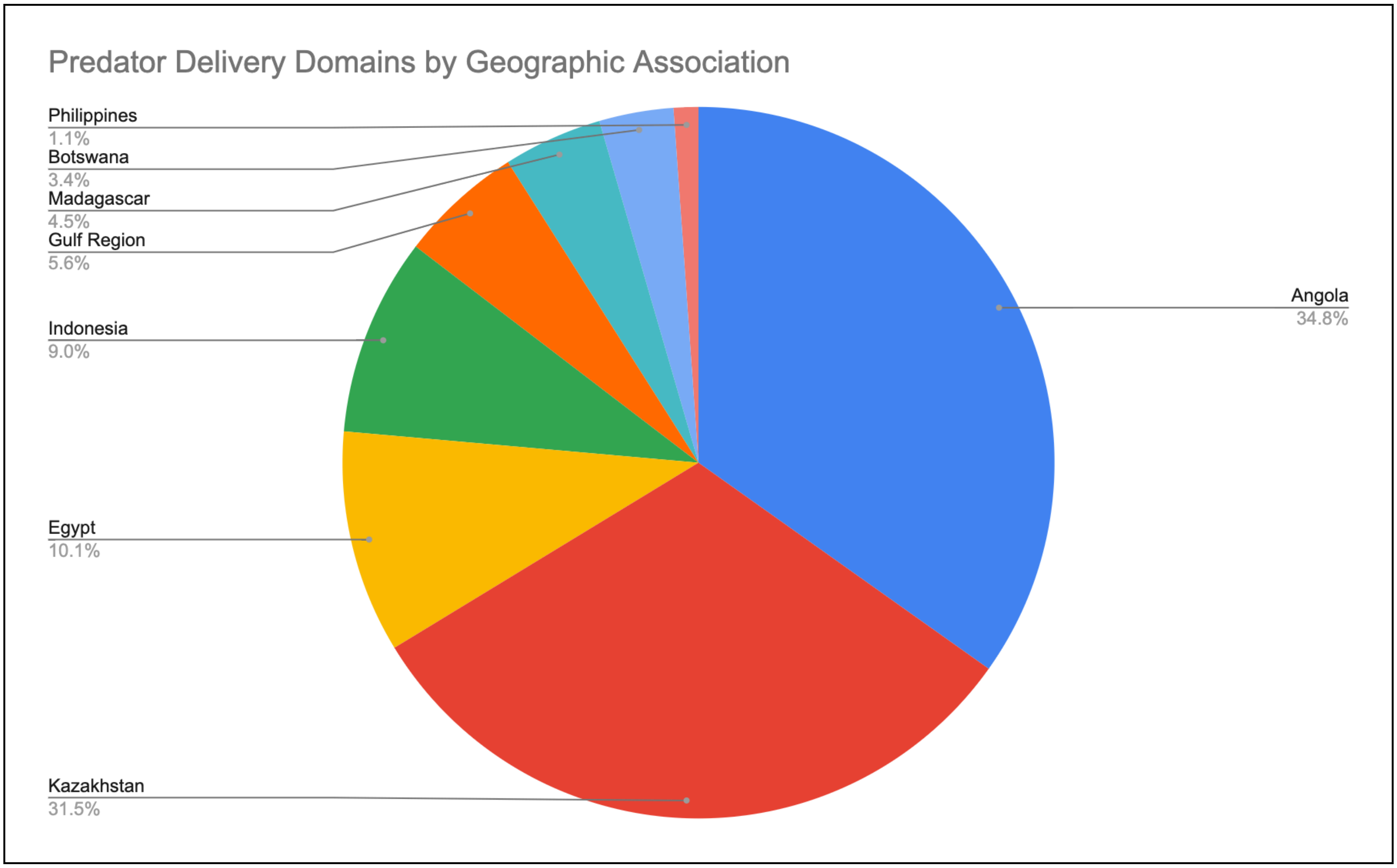

Figure 3: *Predator delivery domains by geographic association (Source: Recorded Future)*

Some notable examples tied to specific countries highly likely spoofing specific organizations are outlined below. Alongside the domain naming analysis, Recorded Future Network Intelligence demonstrated a tiered network architecture connecting the respective delivery servers hosting these domains to suspected customer infrastructure. More details are provided in the “Network Intelligence” section:

Kazakhstan

The domains *krisha-kz[.]com* and *kollesa[.]com* appear to be spoofing Kazakh real estate company “Крыша” (*krisha[.]kz*) and Kazakh auto sales platform “Колёса” (*kolesa[.]kz*). Kazakhstan's record of using cyber surveillance vendors such as NSO Group, FinFisher, and RCS Lab to target activists and politicians further suggests that it’s likely a Predator customer. Notably, over half of the domains revealing distinct ties to countries or regions were linked to Kazakhstan, suggesting a potentially heightened activity level (see **Figure 4**).

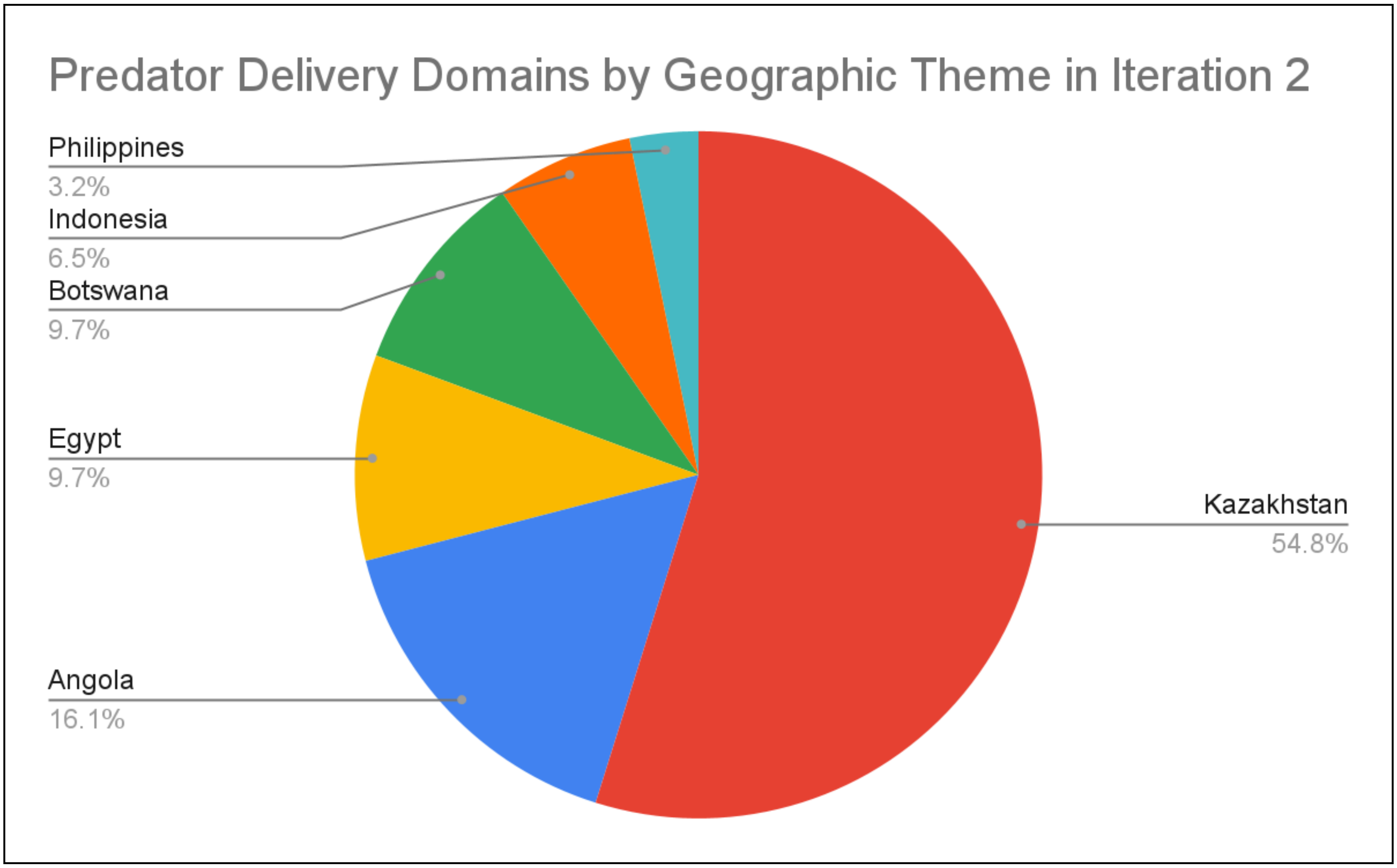

Figure 4: *Predator delivery domains by geographic association in "Iteration 2" (Source: Recorded Future)*

Botswana

The domain *mmegi[.]co* appears to be spoofing "Mmegi Online" (*mmegi[.]bw*), a Botswana-based daily newspaper. In addition, *bw-guardian[.]com* is possibly spoofing the online edition of "Botswana Guardian and The Midweek Sun" (*guardiansun[.]co[.]bw*), Botswana's leading and oldest newspapers. Using the Botswana top-level domain (TLD) in the spoofed domain has been observed in previous instances of Predator delivery domains. For example, *guardian-tt[.]me* associated with Predator operations linked to Trinidad and Tobago seemed to be spoofing The Trinidad and Tobago Guardian (*guardian[.]co[.]tt*) by including the Trinidad and Tobago TLD in the spoofed domain. Although reports have discussed surveillance technology being deployed in Botswana, prior to this, no customers using Predator in Botswana had been identified.

Indonesia

The domain *suarapapua[.]co* appears to be spoofing Suara Papua (*suarapapua[.]com*), a Papua and West Papua province newspaper in Indonesia. Papua and West Papua provinces have a history of press freedom issues, with instances of imprisoning journalists and dissidents. Insikt Group had previously reported on *suarapapua[.]net* in connection to Predator operations. Additionally, other researchers have suggested that Indonesian intelligence services may have acquired and utilized Predator for political surveillance within autonomist movements. Previously, the domains *suarajubi[.]net* and *suarajubi[.]com* were linked to Predator operations, both likely typosquatting Jubi TV, an opposition media outlet in the West Papua province funded by Victor Mambor, a journalist and Papuan autonomy activist.

Egypt

The domain *yo-um7[.]com* appears to be spoofing "Youm7" (*youm7[.]com*), a privately owned Egyptian daily newspaper, which had been spoofed in previous Predator operations. Since Egypt is a known customer of Predator and the spyware has been observed being delivered through network injection from a device physically located in Egypt, Citizen Lab could confidently claim that the Egyptian government was using Predator.

Network Intelligence

Tiered Delivery Network Architecture

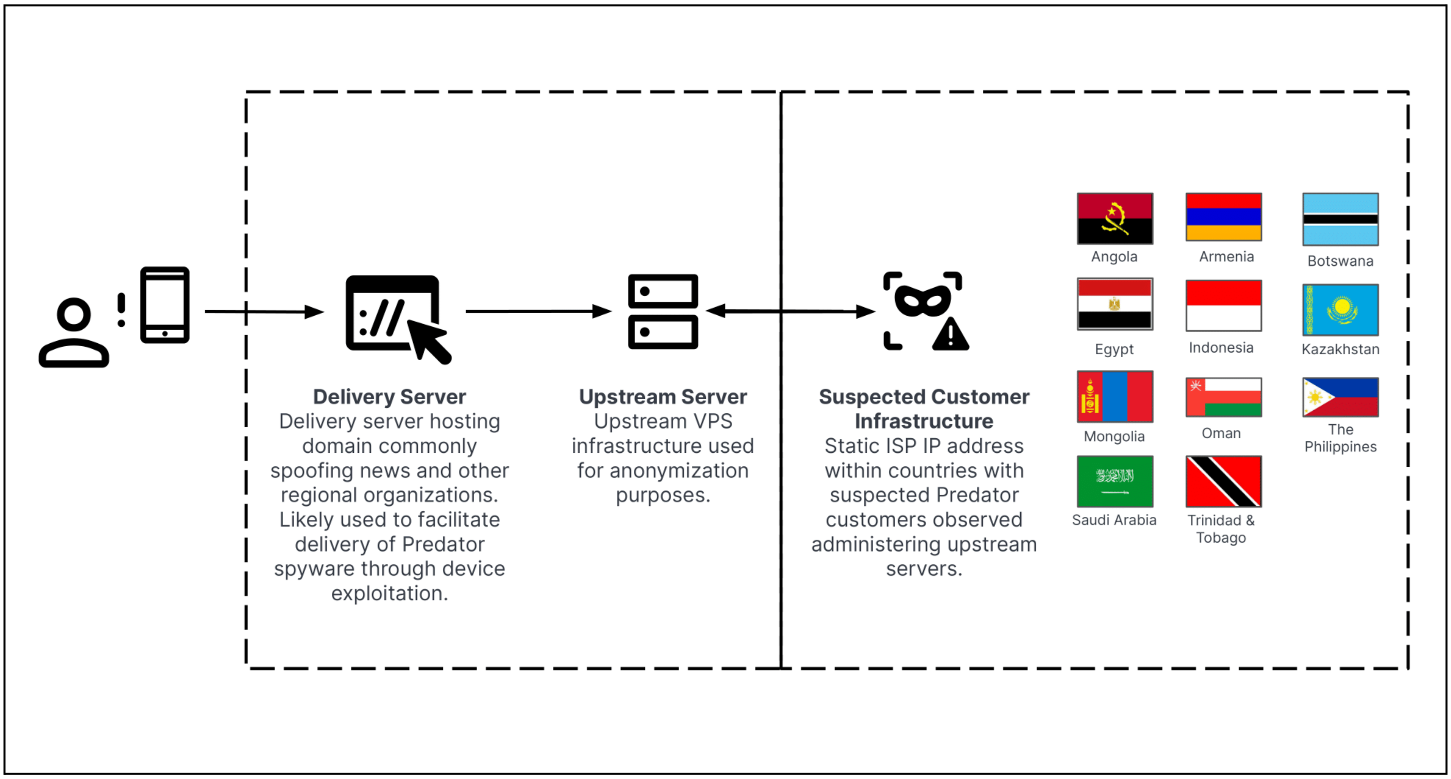
Delivery Server
Delivery server hosting domain commonly spoofing news and other regional organizations. Likely used to facilitate delivery of Predator spyware through device exploitation.
Upstream Server
Upstream VPS infrastructure used for anonymization purposes.
Suspected Customer Infrastructure
Static ISP IP address within countries with suspected Predator customers observed administering upstream servers.
Angola
Armenia
Botswana
Egypt
Indonesia
Kazakhstan
Mongolia
Oman
The Philippines
Saudi Arabia
Trinidad & Tobago

Figure 5: *Multi-tier Predator delivery network architecture (Source: Recorded Future)*

As displayed in **Figure 5**, Insikt Group identified Predator customers using a multi-tiered infrastructure network, very likely to facilitate targeting specific individuals or entities. This network also resembles the high-level network architecture described in the October 2023 Amnesty report. First, we observed the use of downstream delivery servers similar to those described in historical Citizen Lab and Sekoia research; these servers are likely used for device exploitation and initial access. As noted, these servers typically host a domain spoofing particular entities that may be of interest to the target for social engineering purposes.

Using Recorded Future Network Intelligence, these delivery servers were observed regularly communicating with a consistent upstream virtual private server (VPS) IP address over Transmission Control Protocol (TCP) port 10514. These upstream servers are very likely used as hop points for anonymization purposes, reducing the likelihood of associating delivery servers with specific Predator customers.

Furthermore, we identified similar regular communication over TCP port 10514 between these upstream servers and static in-country internet service provider (ISP) IP addresses that we assess are very likely associated with Predator customers. We also regularly observed connections from the in-country ISP IP address to the upstream server using Secure Shell (SSH). In all analyzed instances, delivery servers and associated upstream servers appeared to be dedicated to a single customer.

In several cases, domains hosted on delivery servers clearly associated with specific countries were ultimately administered by a fixed ISP IP address within that particular country via the associated upstream server. Based on our findings and the fact that organizations in these countries were almost all historically reported to be Predator customers, it is highly likely these organizations will very likely continue to employ Predator spyware.

Identification of Victims

At this time, we have not identified specific victims or targets of this latest Predator activity. Since Predator spyware is typically delivered to individual victim devices via vulnerability exploitation, identifying targets is challenging without direct access to those devices in a manner similar to recent Citizen Lab research on Predator activity in Egypt. Victim devices will also typically use dynamic IP addresses within cellular data networks or residential ISP networks when connected to WiFi, which are not commonly attributable to specific individuals without additional information from those service providers. Furthermore, while the identified infrastructure is very likely associated with Predator delivery, whether final-stage Predator implants typically communicate to distinct C2 infrastructure separate from delivery servers is unclear. Predator would likely implement this communication to allow for greater operational security and compartmentalization.

Notably, we observed a number of IP addresses associated with Kazakh mobile network IP ranges communicating with the Predator delivery server *193.29.104[.]13*, which hosted the domain *gabzmus[.]com* at the time of this activity. Additionally, some of the observed delivery domain themes may also offer hints into prospective targeting, such as the repeated spoofing of the Indonesian Papua and West Papua province newspaper Suara Papua, which regularly publishes investigative reporting on human rights issues in these regions. Both activists and journalists in Papua and West Papua have allegedly been subject to restrictions, arrest, and intimidation in recent years.

Considerations on Infrastructure Provisioning

To avoid negative reputations and emphasize their non-accountability for customers' actions involving Predator spyware, Intellexa focuses on cultivating plausible deniability. According to leaked documents, the customer is apparently responsible for both the infrastructure and anonymization (in other words, "Cloud services, domains and anonymization chain which will be provided and managed by customer"). However, based on the wording in these documents, whether the infrastructure is both provided and managed by the customer or whether it is provided by Intellexa and subsequently handed over to the customer for management is not clear.

While providing the infrastructure would grant Intellexa greater control over the attack chain and potentially enhance the product's user-friendliness, it would also afford Intellexa some insight into the targets of their customers, such as specific organizations being spoofed. As a result, maintaining plausible deniability may become less feasible. Although this analysis could not definitively ascertain whether the infrastructure is supplied by Intellexa, a few observations stand out:

- As discussed in the “Domain Naming Theme Analysis” section, a notable level of consistency exists in domain naming patterns, including broader themes like the impersonation of news outlets and more specific elements such as incorporating country International Organization for Standardization (ISO) codes (for example, *bw-guardian[.]com*). While such patterns do not necessarily indicate that the domains have been acquired by a single entity, they do suggest the likelihood of a general recommendation, such as best practices for effective phishing.
- We have observed instances where domains (such as *kejoranews[.]net* and *mb-ph[.]net*) were acquired on the same day through the same registrar (cnobin), utilizing identical *swiftydns[.]com* nameservers, and were linked to customers in various countries. While this similarity could be a coincidence, it appears improbable considering the aforementioned factors.
- Although we have observed identical Statement of Account (SOA) email addresses associated with domains used within the same clusters, we have not identified the use of the same email addresses for domains belonging to different clusters. Therefore, SOA emails aid in identifying infrastructure but cannot be used to confirm the centralized provisioning of that infrastructure.
- On several occasions, we identified delivery domains associated with multiple distinct Predator customers resolving to IP addresses within the same /22 and /24 subnets. This activity is unlikely to have occurred independently and is likely indicative of some level of influence from Intellexa in relation to infrastructure provisioning. Intellexa’s influence could range from directly provisioning this infrastructure to supplying its customers with approved hosting providers and resellers for use in Predator operations.

Outlook

Insikt Group found evidence suggesting ongoing use of Predator in at least eleven countries. Although Predator operators respond to public reporting by altering certain aspects of their infrastructure, they seem to persist with minimal alterations to their modes of operation; these include consistent spoofing themes and focus on types of organizations, such as news outlets, while adhering to established infrastructure setups. While these patterns are relatively easy for threat researchers to identify, these TTPs are presumably producing satisfactory results, eliminating the need for changes. The proliferation and use of Predator and other spyware products, along with hack-for-hire services, outside of serious crime and counterterrorism law enforcement contexts will remain a substantial threat to various organizations and individuals.

Appendix A — Indicators of Compromise

```
Domains:
02s[.]co
06g[.]co
09a[.]co
2-gis[.]kz
astanapark[.]com
beroxe[.]com
buildneeds[.]net
bw-guardian[.]com
cabinet-salyk[.]kz
centent-management[.]net
clazc[.]com
coazoa[.]com
copy-note[.]net
corporatebusinesssolution[.]net
dzhabarzan[.]com
e-kgd[.]kz
ehudaldaa[.]com
escortbabesluxo[.]com
eventnews[.]live
fast-notify[.]com
fastnews[.]biz
fr-monde[.]com
gabzmus[.]com
get-location[.]com
get-location[.]net
highclub[.]life
informationrank[.]net
jumia-egy[.]com
kapital-news[.]com
kejoranews[.]net
kollesa[.]com
krisha-kz[.]com
kroal[.]com
ladiesclubhouse[.]com
lusofonia-mundo[.]com
magnum-kz[.]com
mastershop[.]biz
mb-ph[.]net
mmegi[.]co
msbsck[.]com
mujmbosnoticias[.]com
mundodenoticias[.]online
myfawry[.]net
nospam[.]kz
notify-service[.]biz
nur-news[.]com
olimpbets[.]kz
ongsworld[.]com
```

```
pelovkin[.]com
people-beeline[.]com
peticaonline[.]com
plastictoysworld[.]com
plinkypong[.]com
post-notify[.]info
qazsporttv[.]com
rcuples[.]com
rozavetrovv[.]com
schedulefestival[.]com
shoxtek[.]com
soccer-bw[.]com
spacsaver[.]info
sportnow[.]news
suarapapua[.]co
sustanbuild[.]com
thintank[.]co
tickets-kz[.]com
tobupmi[.]com
tohna[.]net
ulstur[.]co
vendaswebs[.]com
vestinfo[.]net
vestinfo[.]org
vestinfos[.]net
vinho-online[.]com
vlast-news[.]com
walatparez[.]com
weekendcool[.]com
yo-um7[.]com
zakorn[.]com
zikolo[.]net
ztb-news[.]com
```

IP Addresses:

```
2.58.15[.]58
5.39.221[.]36
5.39.221[.]47
5.39.221[.]48
5.255.88[.]172
23.137.248[.]95
37.120.222[.]115
45.129.0[.]125
45.148.244[.]5
45.86.163[.]77
45.86.163[.]93
46.246.97[.]245
46.249.49[.]230
46.30.190[.]98
79.110.52[.]179
79.110.52[.]196
79.137.199[.]216
79.141.175[.]146
```

```
84.247.51[.]14
84.247.51[.]18
85.17.9[.]21
85.17.9[.]73
85.17.9[.]74
85.239.34[.]174
87.121.45[.]29
87.121.45[.]42
87.121.45[.]45
88.119.161[.]135
91.241.93[.]165
95.141.34[.]222
98.142.254[.]112
101.99.75[.]197
141.94.122[.]19
146.70.158[.]144
146.70.161[.]50
158.58.172[.]3
164.215.103[.]143
164.215.103[.]20
169.239.128[.]137
169.239.129[.]48
169.239.129[.]63
169.239.129[.]76
169.255.59[.]98
176.124.198[.]52
176.124.198[.]55
185.113.8[.]67
185.113.8[.]83
185.117.91[.]165
185.117.91[.]237
185.130.227[.]29
185.130.227[.]88
185.130.227[.]95
185.130.45[.]34
185.130.46[.]165
185.130.46[.]202
185.156.172[.]17
185.156.172[.]20
185.156.172[.]48
185.158.248[.]131
185.158.248[.]85
185.196.9[.]76
185.212.47[.]75
185.219.220[.]99
185.219.221[.]30
185.62.58[.]107
185.66.140[.]112
192.46.237[.]163
193.168.143[.]111
193.168.143[.]116
193.168.143[.]184
193.168.143[.]185
```

```
193.233.161[.]137
193.233.161[.]163
193.29.104[.]13
193.29.104[.]5
193.29.104[.]83
193.29.59[.]171
193.42.36[.]106
193.42.36[.]84
212.237.217[.]127
213.252.246[.]152
```

Appendix B — Predator Delivery Servers

Domain	IP Address	First Seen	Last Seen
06g[.]co	185.130.227[.]29	2023-12-22	2024-02-21
02s[.]co	185.130.227[.]95	2023-12-22	2024-02-21
spacsaver[.]info	45.148.244[.]5	2023-11-30	2024-02-20
09a[.]co	5.39.221[.]36	2023-12-22	2024-02-21
ongsworld[.]com	146.70.158[.]144	2023-11-16	2024-02-21
fr-monde[.]com	169.239.129[.]76	2023-12-15	2024-02-20
lusofonia-mundo[.]com	169.239.129[.]63	2023-12-15	2024-02-17
ladiesclubhouse[.]com	169.239.129[.]48	2023-12-15	2024-02-18
vinho-online[.]com	169.239.128[.]137	2023-12-15	2024-02-17
vendaswebs[.]com	185.158.248[.]131	2023-11-16	2024-02-17
mundodenoticias[.]online	185.196.9[.]76	2023-11-16	2024-02-17
mujmbosnoticias[.]com	185.212.47[.]75	2023-11-02	2024-02-21
soccer-bw[.]com	185.130.46[.]165	2023-11-22	2024-02-17
mmegi[.]co	45.129.0[.]125	2023-11-22	2024-02-16
bw-guardian[.]com	95.141.34[.]222	2023-11-19	2024-02-17
yo-um7[.]com	185.130.46[.]202	2023-11-29	2024-02-17
sustanbuild[.]com	193.29.104[.]5	2023-11-25	2024-02-17
myfawry[.]net	2.58.15[.]58	2023-12-14	2024-02-20
jumia-egy[.]com	79.110.52[.]196	2023-12-14	2024-02-17
suarapapua[.]co	158.58.172[.]3	2023-12-01	2024-01-29
kejoranews[.]net	185.158.248[.]85	2023-12-07	2024-02-15
nospam[.]kz	176.124.198[.]52	2023-12-28	2024-02-13
olimpbets[.]kz	176.124.198[.]55	2023-12-28	2024-02-13

vlast-news[.]com	185.156.172[.]20	2023-12-08	2024-02-16
ztb-news[.]com	185.156.172[.]17	2023-12-08	2024-02-17
cabinet-salyk[.]kz	185.156.172[.]48	2023-12-15	2024-02-21
zikolo[.]net	193.168.143[.]116	2023-11-11	2024-02-14
magnum-kz[.]com	45.86.163[.]93	2023-12-08	2024-02-20
tickets-kz[.]com	45.86.163[.]77	2023-12-10	2024-02-17
people-beeline[.]com	5.39.221[.]47	2023-12-14	2024-02-17
rozavetrovv[.]com	5.39.221[.]48	2023-12-14	2024-02-17
2-gis[.]kz	79.137.199[.]216	2023-12-28	2024-02-20
e-kgd[.]kz	85.17.9[.]21	2023-12-15	2024-02-17
kapital-news[.]com	85.17.9[.]73	2023-12-14	2024-02-19
nur-news[.]com	85.17.9[.]74	2023-12-14	2024-02-21
astanapark[.]com	87.121.45[.]42	2023-12-11	2024-02-16
krisha-kz[.]com	88.119.161[.]135	2023-11-26	2024-02-17
ehudaldaa[.]com	84.247.51[.]14	2023-12-23	2024-02-20
ulstur[.]co	84.247.51[.]18	2023-12-25	2024-02-20
mb-ph[.]net	193.42.36[.]106	2023-12-07	2024-02-21
buildneeds[.]net	141.94.122[.]19	2023-11-21	2024-02-17
sportnow[.]news	185.113.8[.]67	2023-11-11	2024-02-19
corporatebusinesssolution[.]net	193.168.143[.]184	2023-11-25	2024-02-09
informationrank[.]net	193.168.143[.]185	2023-11-25	2024-02-17
centent-management[.]net	193.29.59[.]171	2023-11-21	2024-02-09
highclub[.]life	46.249.49[.]230	2023-11-11	2024-02-21
vestinfos[.]net	185.130.45[.]34	2023-12-22	2024-02-09
get-location[.]net	46.246.97[.]245	2023-12-21	2024-02-08
vestinfo[.]org	79.141.175[.]146	2023-12-22	2023-12-22

eventnews[.]live	185.219.221[.]30	2023-12-04	2024-02-08
get-location[.]com	192.46.237[.]163	2023-12-04	2024-02-20
vestinfo[.]net	87.121.45[.]29	2023-12-04	2024-02-17
thintank[.]co	5.255.88[.]172	2023-10-25	2024-01-20
fastnews[.]biz	101.99.75[.]197	2023-11-17	2024-02-18
plinkypong[.]com	146.70.161[.]50	2023-11-29	2024-02-17
peticaonline[.]com	164.215.103[.]143	2023-11-27	2024-02-17
escortbabesluxo[.]com	164.215.103[.]20	2023-11-03	2024-02-13
coazoa[.]com	169.255.59[.]98	2023-11-01	2024-02-19
weekendcool[.]com	185.113.8[.]83	2023-11-18	2024-02-14
qazsporttv[.]com	185.117.91[.]237	2023-12-14	2024-02-17
pelovkin[.]com	185.117.91[.]165	2023-11-29	2024-02-14
plastictoysworld[.]com	185.130.227[.]88	2023-11-28	2024-02-17
tohna[.]net	185.219.220[.]99	2023-11-02	2024-02-10
notify-service[.]biz	185.62.58[.]107	2023-11-16	2024-02-01
copy-note[.]net	185.66.140[.]112	2023-11-29	2024-01-31
zakorn[.]com	193.168.143[.]111	2023-11-10	2024-02-17
walatparez[.]com	193.233.161[.]137	2023-12-09	2024-02-17
tobupmi[.]com	193.233.161[.]163	2023-11-14	2024-02-16
gabzmus[.]com	193.29.104[.]13	2023-11-14	2024-02-17
msbsck[.]com	193.29.104[.]83	2023-11-16	2024-02-17
mastershop[.]biz	193.42.36[.]84	2023-11-17	2024-02-11
kollesa[.]com	212.237.217[.]127	2023-11-10	2024-02-17
schedulefestival[.]com	213.252.246[.]152	2023-11-16	2024-02-18
post-notify[.]info	23.137.248[.]95	2023-11-17	2024-02-17
dzhabarzan[.]com	37.120.222[.]115	2023-12-08	2024-02-21

shoxtek[.]com	46.30.190[.]98	2023-11-23	2024-02-12
fast-notify[.]com	79.110.52[.]179	2023-12-09	2024-02-19
clazc[.]com	85.239.34[.]174	2023-11-24	2024-02-17
beroxe[.]com	87.121.45[.]45	2023-12-09	2024-02-21
kroal[.]com	91.241.93[.]165	2023-12-08	2024-02-19
rcuples[.]com	98.142.254[.]112	2023-11-28	2024-02-02

Table 2: *Predator delivery domains from “Iteration 2” with associated IP addresses (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

Table 3: *Mitre ATT&CK techniques observed (Source: Recorded Future)*

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 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com