Active Lycantrox infrastructure illumination

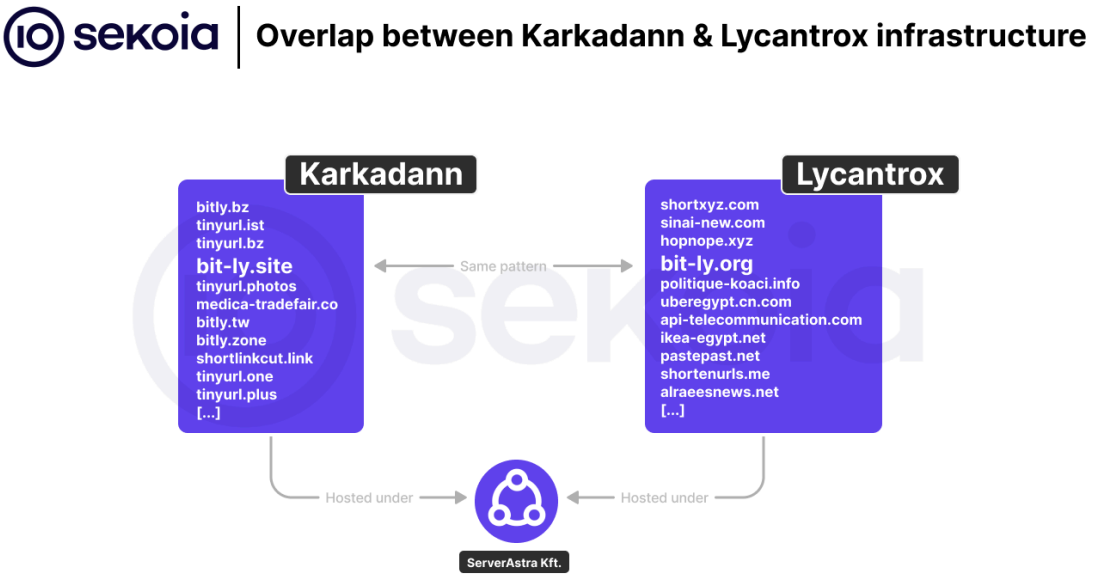
By Felix Aimé, Maxime A. and Sekoia TDR

Published: 2023-10-02 · Archived: 2026-04-05 22:46:34 UTC

On September 22, Citizenlab published a blog post regarding the use of **Cytrox's signature Predator spyware** against the iPhone of **the former Egyptian MP Ahmed Eltantawy**. In August and September 2023, Ahmed Eltantawy was targeted via **network-based injection**, redirecting him to malicious web pages when he visited non-HTTPS sites, by exploiting a zero-day exploit chain (CVE-2023-41991, CVE-2023-41992, CVE-2023-41993) used to install Predator on iOS versions up to 16.6.1.

Cytrox has previously attracted attention for its involvement in the development of its **Predator spyware for targeting civil society**. CitizenLab and META have released a few blog posts and reports delving into Cytrox and its affiliated cyber intelligence consortium, known as **Intellexa**.

In December 2021, **we issued a FLINT report exploring potential connections between Cytrox customers** (that we track under the ***Lycantrox*** intrusion set) of and **Candiru customers** (tracked under the ***Karkadann*** intrusion set), prompted by similarities in the infrastructure employed by their respective clientele to compromise their targets. This overlapping infrastructure may stem from shared customers utilizing both Cytrox and Candiru technologies.



SEKOIA.IO is actively monitoring **hundreds of malicious infrastructure clusters** to protect its customers. In light of the recent Citizenlab blogspot and in solidarity with the efforts against cyber mercenaries, we have chosen to shed light on one of the infrastructure clusters employed by *Lycantrox*, potentially for compromising their targets.

While **the domain patterns look like entry points for exploits kits**, the scale of this infrastructure suggests a broader use of it. However, we lack concrete evidence to confirm this.

Infrastructure illumination

The infrastructure used by the *Lycantrox* consists of **VPS hosted in several autonomous systems**. Each *Lycantrox* user seems to run his own instances of VPS and manage his own domain name related to it. When looking precisely at the services listed on the instances, most of the time there are two open ports, the SSH used for the administration and a 443 managed by Nginx. On several occasions, only the 443 is available.

Unlike most of the C2s listening on 443 out there, **the Nginx instance is configured to answer a certificate only if a valid domain name is provided** to it, otherwise it will answer a SSL_ERROR_UNRECOGNIZED_NAME_ALERT and the connexion will be dropped.

To correlate the infrastructure, we can simply get all the IP addresses with the previously disclosed heuristic, looking for VPS with two open ports or less. This will provide us a list of hundreds of IP addresses that we will then be able to check against a passive DNS database in order to grab some domain names to test.

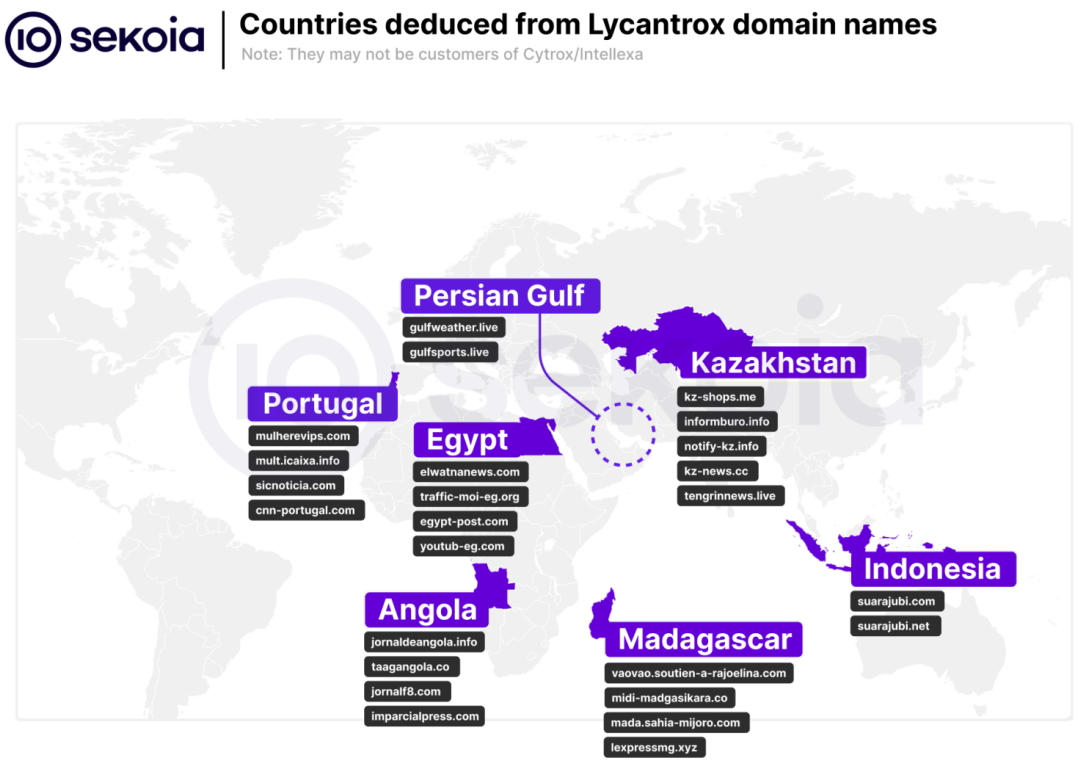
Only by looking at the domain names resolving this list, we can spot a few that ring a bell to us when hunting historically with *Lycantrox* infrastructures such as **fake URL shorteners** or **typosquatting news websites** such as bitshort[.]info or elwatnanews[.]com. Moreover, many of them are linked to name servers that are known to accept cryptocurrency payments and be associated with cyber criminal activities. However, we need to be sure of their use by *Lycantrox*.

To ensure that the mentioned domains are related to *Lycantrox* infrastructure, an active check can be done. The aim of that is to discover if some of them present anomalies that a default Nginx installation doesn’t show, which will be another discriminant thing to add to our final heuristic. During our investigation we found that the domains answered to any tested URL with a 204 No Content status code even if they showed a 404 error page, allowing us to categorize each of them, *Lycantrox* related or non-*Lycantrox* related.

At the end, **121 unique active domain names were found** being related with high confidence to an infrastructure cluster linked to the *Lycantrox* intrusion set. Some of the discovered domains typo squat or have few references to specific geographical areas shown in the following map.

We are also providing under “medium confidence” suspected *Lycantrox* related domain names that we haven’t been able to check actively during the investigation. **It is worth noting that, by poking around them it’s possible to see other domains that might be related to the same threat actors**, possibly used in the past or as backup infrastructure.

Context analysis



Madagascar

The only servers using subdomains pointing to the servers that answered to our heuristic are related to Madagascar. These websites (soutien-a-rajoelina[.]com, emergence-mada[.]com and sahia-mijoro[.]com) – **which seem to have been created by the threat actor itself** – are wordpress blogs containing real articles taken from the Madagascan newspaper Midi Madagasikara, which is also typostatted as midi-madgasikara[.]co.

Even if their sub domains are pointing to malicious servers, we haven't been able to detect any malicious iframes, script insertions or fingerprinting scripts leading to the malicious servers on the websites. While looking in open sources for references to these domains, we've seen only one occurrence of emergence-mada[.]com – **a post of this blog was linked in a Facebook group supporting the actual president**, Andry Nirina Rajoelina. Sekoia.io was not able to observe malicious content in the history of the linked webpage.

Madagascar is currently campaigning for a **presidential election** on **9 November 2023**, where Rajoelina, current president elected in 2018 is seeking its reelection. Sekoia.io assess it is **plausible Madagascar government services** – such as police or domestic intelligence – did **purchase and leverage Cytrox's Predator** malware to **conduct political domestic surveillance**, months before the election. This hypothesis is politically coherent with Rajoelina's undemocratic approach – 2009 *coup d'etat* getting him in power, 2019 Senat major reform, intense propaganda on social media promoting its reforms. In addition, according to Intelligence Online, the company **Intellexa**, Cytrox's parent company, brought from a french company a **contract with the Madagascar government** for the collection and processing of interception data.

Indonesia

Among the *Lycantrox* domains, suarajubi[.]net and suarajubi[.]com likely typosquat **Jubi TV**, a West Papua province **opposition media** funded by Victor Mambor, journalist and Papuan autonomy activist. Jubi TV often reports Jakarta operations towards Papuan activists. Sekoia.io assess it is possible **Indonesian intelligence**

services purchased and leverage Cytrox's Predator malware to conduct **political surveillance**, at least on autonomist movements.

Kazakhstan

It is not surprising to see Kazakhstan on that list as this country has a troubled history with cyber surveillance vendors such as NSO, RCS Lab or FinFisher to compromise devices belonging to human right activists, politicians, journalists and opponents. Based on the *Lycantrox* domains Sekoia.io investigated and on Astana documented use for cyber surveillance tools, **it is likely Kazakhstan** intelligence services **purchased and use Cytrox's Predator** malware.

Angola

Sekoia.io analysts found several domains associated with Angola entities. At least six of them typosquat online medias – folha-9[.]com, factosdiarios[.]co or lilpastanews[.]co– and several others seems related to national entities (the main telecom operator, the national company for oil production, ministry of finance, the national postal service). Sekoia.io found other typosquatted domains associated with Portugal – mult[.]icaixa[.]info, cnn-portugal[.]com – that we assess as possible part of the Predator campaign in Angola. Given the multiple Angola-related and Portuguese speaking domains, Sekoia.io assess **it is plausible Angola government services were also Cytrox clients**.

Conclusion

It is worth mentioning that *Lycantrox* has hardened its reverse proxies since our previous investigations and after some public disclosures in order to prevent such illumination. However, sometimes, **too much hardening can be discriminatory from a defender point of view**, as we can see with this correlation.

Sekoia.io will continue its efforts against known cyber mercenary threat actors by illuminating their infrastructure and providing for free associated indicators of compromise (IOCs) to the community. Therefore, if you are a **journalist**, **politician** or **human rights activist** we encourage you to check your device for the presence of the following list of domain names, by using, for example **MVT** for analysis of your Android/iOS logs or **SPYGUARD** to check in real time your device's network communications against a set of heuristics to detect possible implant beaconing.

Indicators of compromise

Domains mentioned in the CitizenLabs blogpost, also found during our investigation.

```
betly[.]me
sec-flare[.]com
verifyurl[.]me
```

High confidence, active infrastructure during the time of the investigation

```
candidaturasminfin[.]info
grupohel[.]social
notify-kz[.]info
```

```
intnews[.]world
taagangola[.]co
afrinew[.]net
tupuca[.]co
newsworldsports[.]co
newspool[.]net
informburo[.]info
dealstransfer[.]net
gorlovski[.]com
egypt-post[.]com
podcastnow[.]club
suarajubi[.]net
suarajubi[.]com
pasteposta[.]com
post-kz[.]info
mada[.]sahia-mijoro[.]com
bbitly[.]com
culniks[.]info
folha-9[.]com
shortly[.]work
lttlnk[.]net
mult[.]icaixa[.]info
mujimbos[.]co
leefco[.]net
liveco[.]live
showsme[.]info
brkorage[.]live
clckbck[.]com
flowercafee[.]com
soq[.]one
jornaldeangola[.]info
geloraku[.]id
smallme[.]net
quick-ads[.]com
jofki[.]com
midi-madgasikara[.]co
flytaps[.]com
factosdiarios[.]co
kz-news[.]cc
lilpastanews[.]co
popup-pw[.]info
eventes[.]org
fdnews[.]info
unitei[.]co
businessafricaonline[.]org
breaknews[.]live
actualite[.]emergence-mada[.]com
```

```
candidaturassonangol[.]info
correiosdeangola[.]info
9o[.]gg
allafrika[.]live
visavfsglobal[.]co
adenuncia[.]com
portalxa[.]com
sky-news[.]live
vinhosadega[.]com
shop-collect[.]com
bestwesternt[.]com
traffic-moi-eg[.]org
conodeti[.]com
gulfsports[.]info
dw-news[.]co
lexpressmg[.]xyz
jakalas[.]online
t-ready[.]me
grvnews[.]live
air-shopping[.]net
gostosadeluxo[.]com
aoatlasescort[.]com
universedades[.]com
bitshort[.]info
intercontinentalhg[.]com
clubs-k[.]com
nm-weather[.]live
imparcialpress[.]com
blitzmedia[.]live
shanam[.]org
kz-shops[.]me
youtub-eg[.]com
elwatnanews[.]com
tengrinnews[.]live
jornalf8[.]com
growebservice[.]com
zoometting[.]com
vaovao[.]soutien-a-rajoelina[.]com
ongs[.]life
truelocation[.]org
ordas-kz[.]com
glbnews[.]live
newsreuter[.]com
novojornal[.]co
almasrylayoum[.]com
dhll[.]live
redirto[.]info
```

```
mulherevips[.]com
sicnoticia[.]com
weather-live[.]com
africa-confidentiel[.]fr
skranski[.]com
cnn-portugal[.]com
wesalcity[.]net
platinalines[.]com
onlinewebinarmarketing[.]com
btlin[.]life
tclnk[.]live
kalwaski[.]xyz
sysnet[.]life
clcti[.]net
qamqors[.]net
gorows[.]live
moncn[.]co
skollie[.]online
smcu[.]me
sysly[.]sbs
bulk-ads[.]com
gulfweather[.]live
shortly[.]work
gulfsports[.]live
```

Moderate to high confidence, dormant or inactive infrastructure during the time of the investigation.

```
amritacity[.]com
awlaqf[.]sbs
bosmata[.]com
politi[.]live
toomec[.]net
crudco[.]info
corncog[.]com
dbtest[.]online
espn-sports[.]live
ftlink[.]info
gsxr[.]me
gulfnews[.]today
gulfweather[.]co
helpemail[.]net
isalways[.]net
isconn[.]net
islink[.]info
letmelook[.]one
lnkkdis[.]xyz
```

```
lnklit[.]com
mg-news[.]info
miceups[.]com
mncnn[.]info
mnmlink[.]co
pklnk[.]com
post-info[.]kz
previeweb[.]xyz
sexychats[.]nl
southchinapost[.]net
supasports[.]xyz
syscncc[.]live
tconn[.]net
weatherforecast[.]services
```

Thank you for reading this blogpost. We welcome any reaction, feedback or critics about this analysis. Please contact us on tdr[at]sekoia.io

Feel free to read other TDR analysis here :

Share

APT CTI Cytrox Predator

Share this post:
