



# Stately Taurus APT Group Targets Asian Countries: What Do the Campaign IoCs Reveal?

## Table of Contents

1. [Executive Report](#)
2. [Appendix: Sample Artifacts](#)

## Executive Report

A decade-old advanced persistent threat (APT) group called “Stately Taurus,” also known as “Mustang Panda” and “Earth Preta,” was recently observed targeting Association of Southeast Asian Nations (ASEAN) countries in cyberespionage activities. Specifically, Palo Alto Networks observed two malware packages that may have been used to target Japan, Myanmar, the Philippines, and Singapore. The threat group used these packages on 4–5 March 2024, around the same days the ASEAN-Australia Special Summit was held.

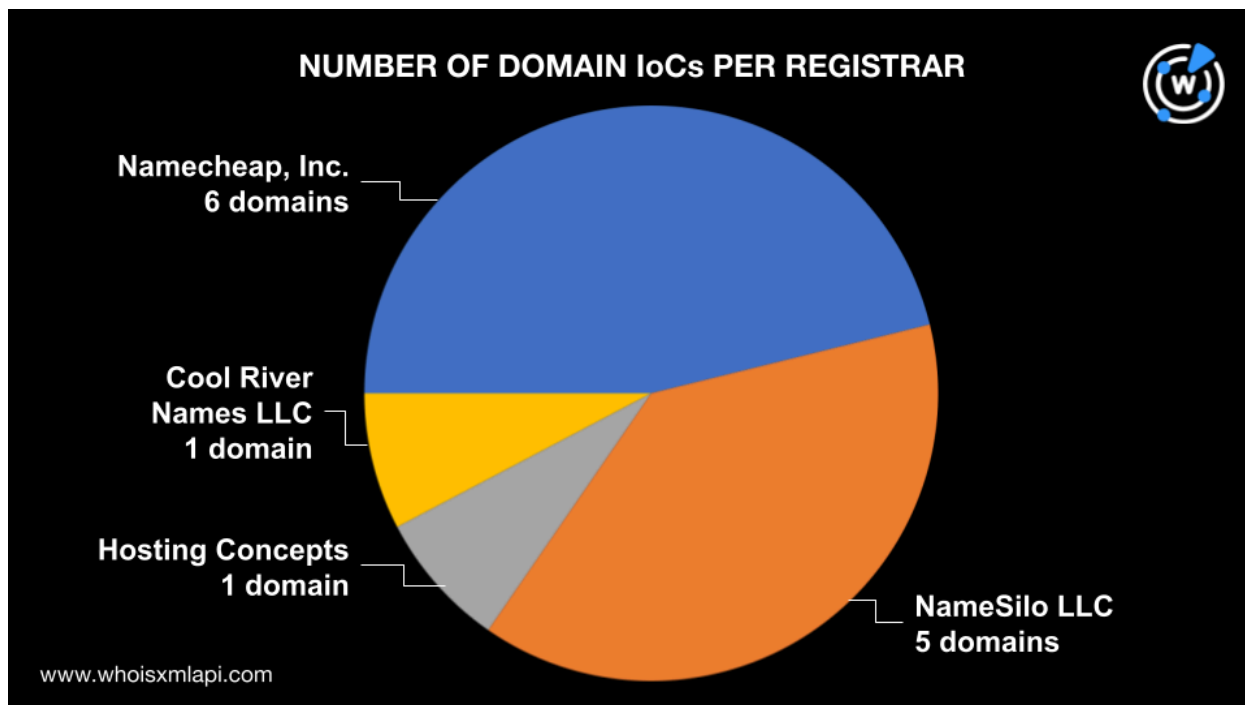
Building on lists of indicators of compromise (IoCs) published by [Palo Alto Networks](#) and [Trend Micro](#) comprising eight subdomains, 13 domains (including six extracted from the subdomains tagged as IoCs), and 15 IP addresses, the WhoisXML API research team uncovered:

- 61 email-connected domains
- Four additional IP addresses
- One IP-connected domain
- 67 string-connected domains

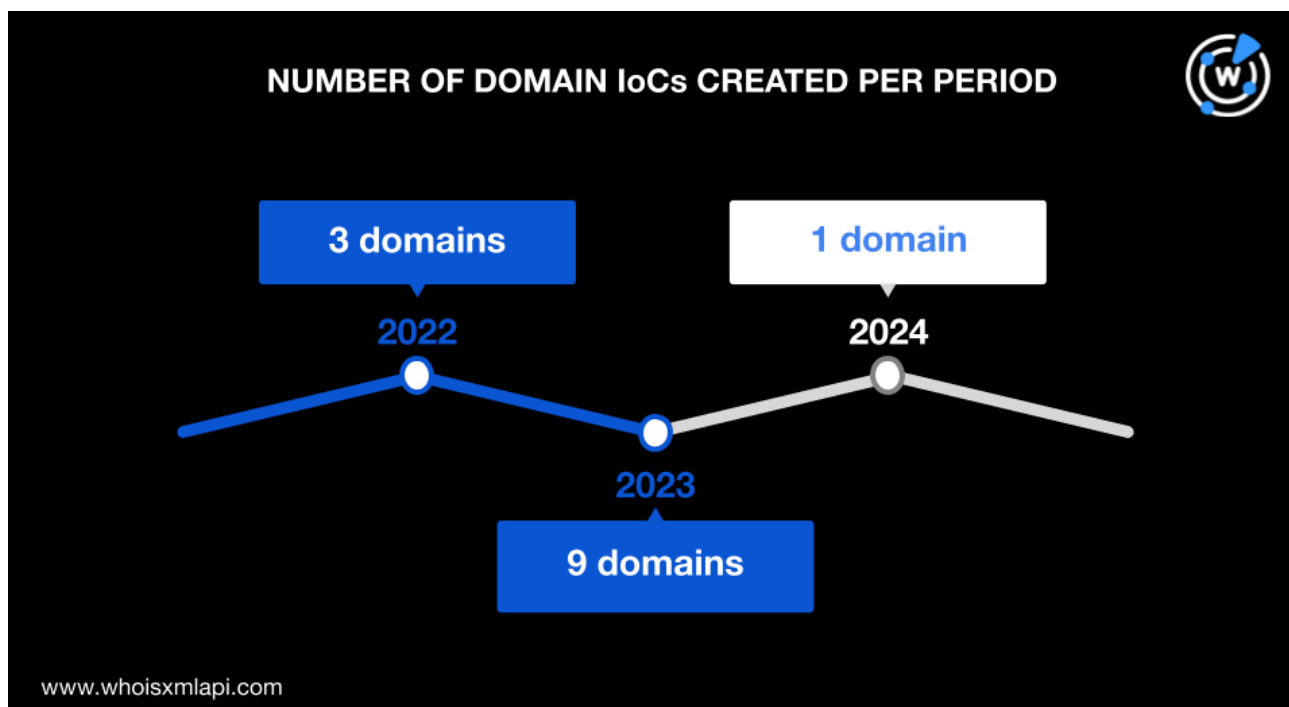
## Stately Taurus IoC Profile and Analysis

When analyzing an attack infrastructure, our usual first step is to gather the WHOIS details of the domains tagged as IoCs. For Stately Taurus, we did a [bulk WHOIS lookup](#) for 13 domains, six of which were extracted from the 8 subdomains found on the IoC list. We uncovered the following details:

- Four registrars administered them—NameCheap, Inc. with six domains; NameSilo LLC with five domains; and Cool River Names LLC and Hosting Concepts with one domain each.

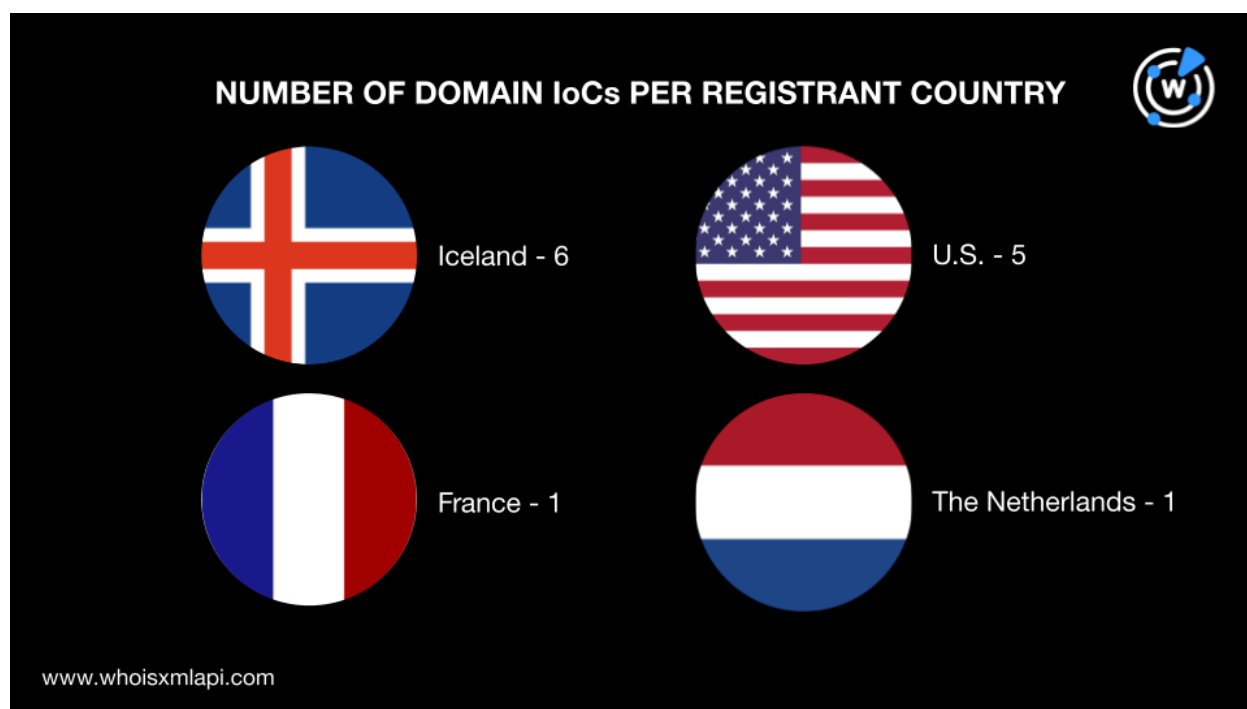


- The oldest domain was registered in August 2022 while the newest was created in February 2024. Nine of the domains were created in 2023, three in 2022, and one in 2024.



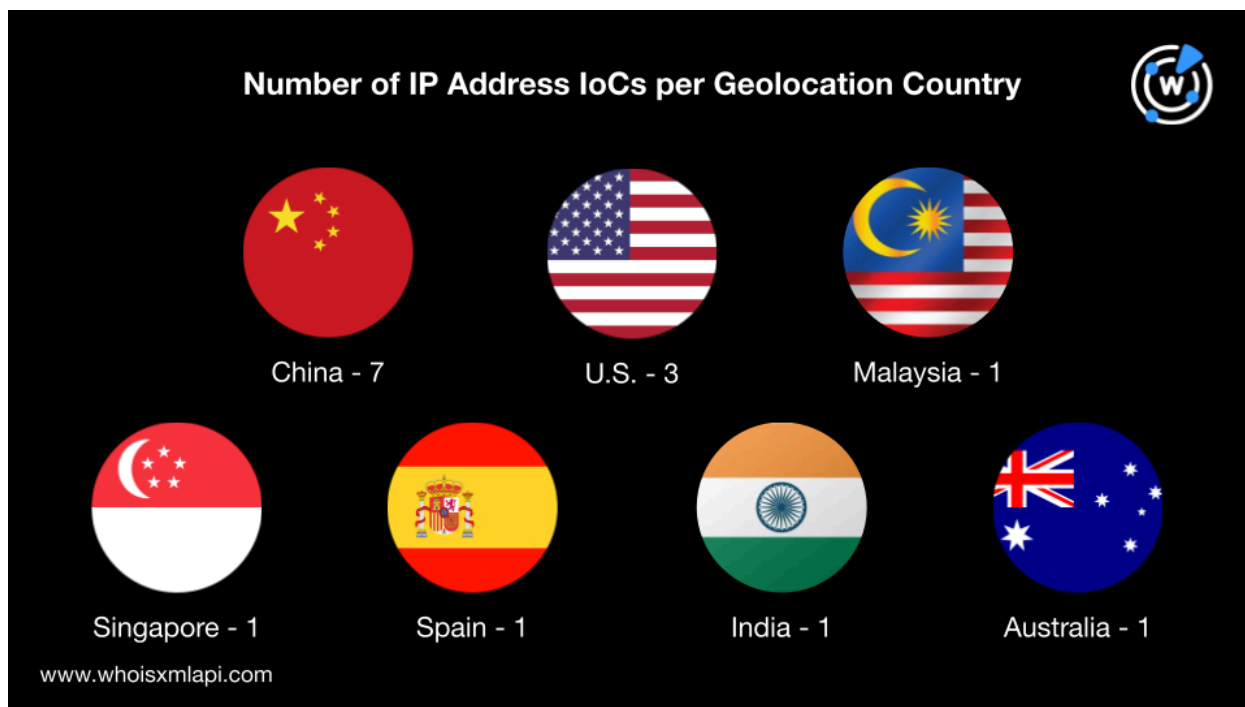


- Their registrations were spread across four registrant countries—six domains in Iceland, five in the U.S., and one each in France and the Netherlands.

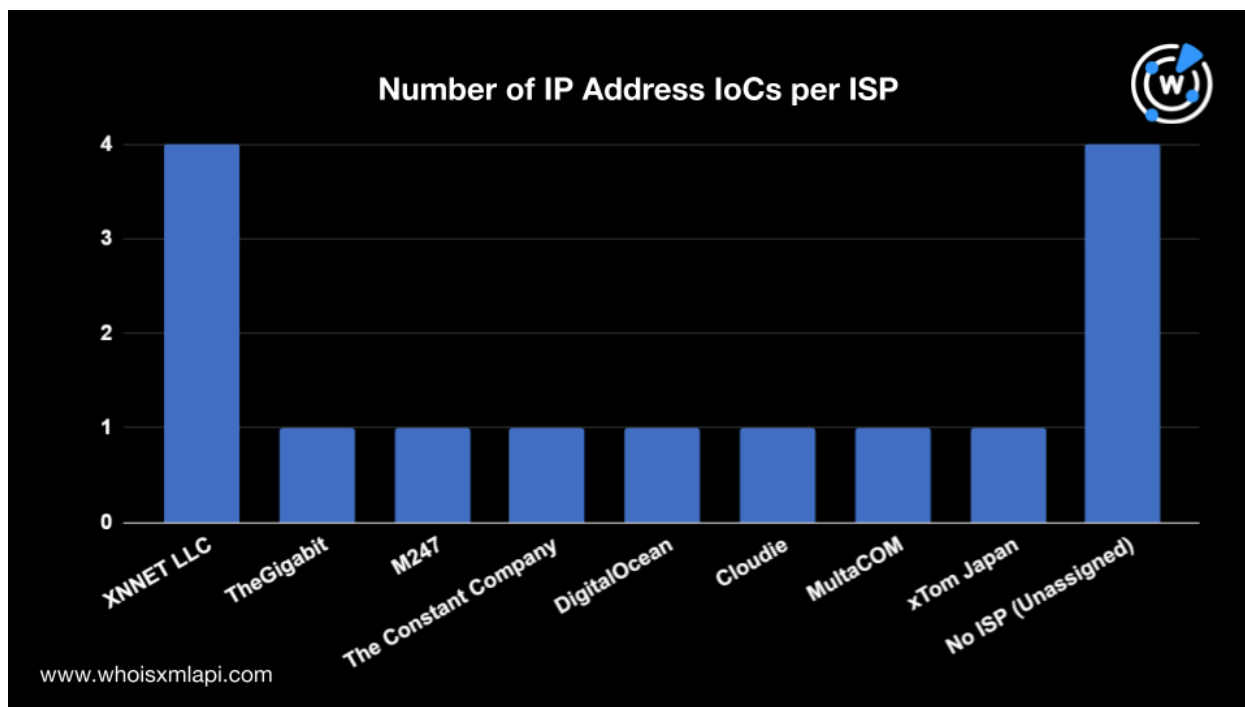


The next step was to subject the 15 IP addresses tagged as IoCs to a [bulk IP geolocation lookup](#), leading us to discover that:

- The IP addresses were geolocated across seven countries. Seven originated from China; three from the U.S.; and one IP address each from Malaysia, Singapore, Spain, India, and Australia.



- They were controlled by eight ISPs. Four IP addresses were under XNNET LLC and one each was administered by TheGigabit, M247, The Constant Company, DigitalOcean, Cloudie, MultaCOM, and xTom Japan. Four IP addresses were possibly unassigned.





## Stately Taurus IoC Expansion

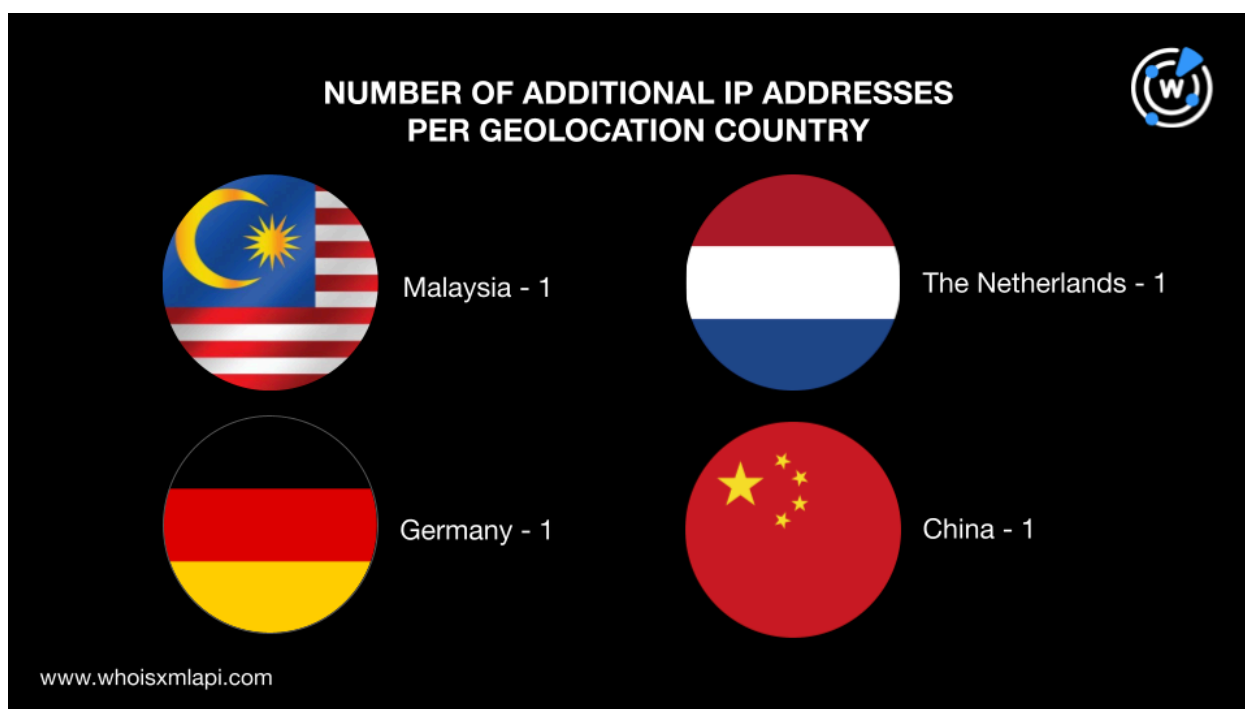
After analyzing the attack infrastructure of the APT group, we expanded the lists of IoCs to obtain additional threat artifacts or web properties that could be connected to Stately Taurus.

[WHOIS History API](#) searches for the domain IoCs led us to discover 38 email addresses in their historical WHOIS records, eight of which were public. [Reverse WHOIS API](#) revealed that these public email addresses appeared in the current WHOIS records of 61 domains.

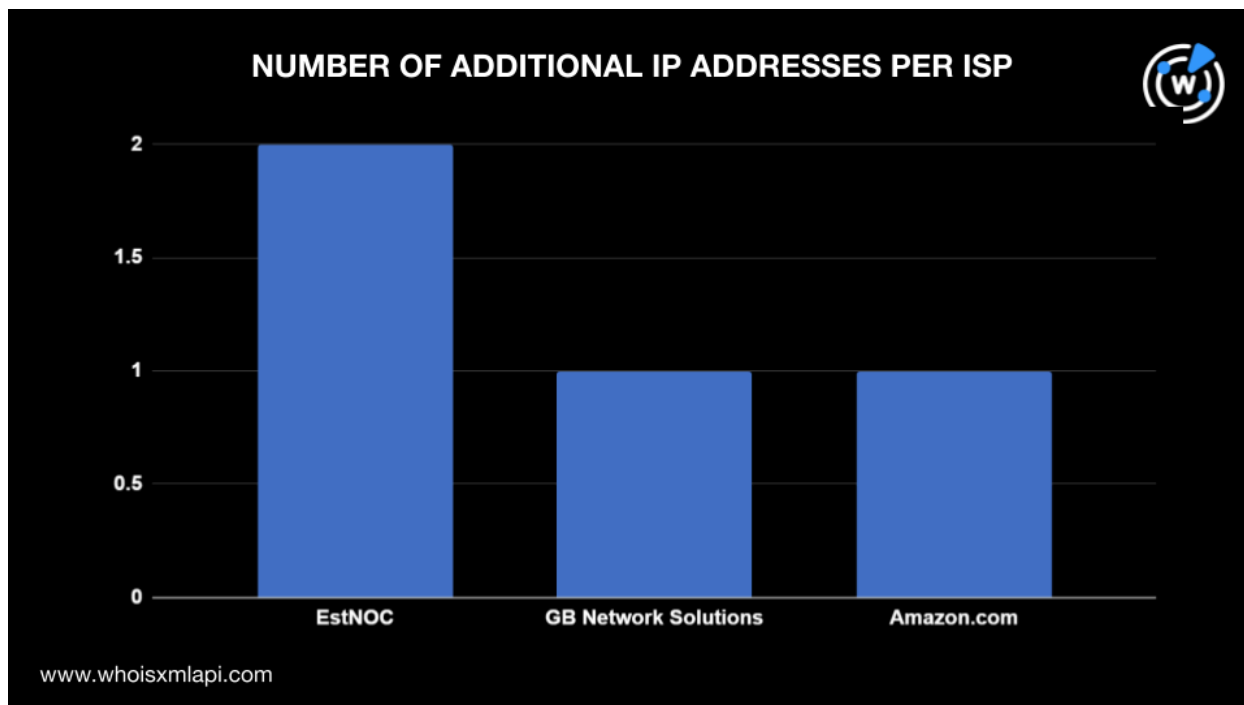
For our next step, we ran [DNS lookups](#) on the seven domains and eight subdomains tagged as IoCs to obtain their IP resolutions. This led us to discover four additional IP addresses.

Performing [IP geolocation lookups](#) on the four IP addresses revealed that:

- They can be traced to different countries, specifically Malaysia, the Netherlands, Germany, and China.



- They were administered by three ISPs. EstNOC managed two IP addresses and GB Network Solutions and Amazon.com controlled one each.



We also ran the four additional IP addresses on [Threat Intelligence API](#), revealing that they were all associated with various threats. The table below shows a couple of examples.

IP ADDRESSES	ASSOCIATED THREAT TYPES
103[.]28[.]91[.]193	Malware
3[.]64[.]163[.]50	Command and control (C2) Phishing Malware Spam

Next, we subjected the 15 IP addresses tagged as IoCs and four additional IP addresses (i.e., 19 IP addresses in total) to [reverse IP lookups](#), which showed that two were potentially dedicated. They led to only one IP-connected domain after removing duplicates, the IoCs, and the email-connected domains.

Finally, we analyzed the IoCs' string usage, focusing on finding other domains containing the text strings used in the domain IoCs. To do that, we used the following search parameters and strings on [Domains & Subdomains Discovery](#) and found 67 string-connected domains.

- Starts with **electric** and contains **tulsa**
- Starts with **iviber**
- Starts with **meet** and contains **viber**



- Contains **viber** and **api**.
- Starts with **getfiledown**
- Starts with **getfilefox**
- Starts with **estmongolia**
- Starts with **openservername**
- Starts with **nerdnooks**
- Starts with **daydreamdew**
- Starts with **comsnews**
- Starts with **bonuscave**
- Starts with **markplay**.

Meanwhile, we noticed that most of the third-level domains of the subdomains tagged as IoCs were generic tech-related terms, such as **images**, **web**, **news**, **ai**, and **www**. A wildcard search on [Threat Intelligence API](#) revealed that these strings that appeared in the IoCs also showed up in hundreds of other IoCs involved in malware, phishing, and various threats. Some examples are shown in the table below.

TEXT STRING	NUMBER OF IoCs CONTAINING THE STRING
<b>images.*</b>	225
<b>web.*</b>	801
<b>news.*</b>	501
<b>ai.*</b>	123
<b>www.*</b>	10,000

A similar search on [Threat Intelligence API](#) using the strings that appeared in the domain IoCs revealed that there are already 31 IoCs containing the string **viber** and 75 starting with the string **getfile**.

Our investigation of the IoCs associated with the recent Stately Taurus APT campaigns began with eight subdomains, 13 domains (six of which were extracted from the subdomains tagged as IoCs), and 15 IP addresses.

After digging through their WHOIS details, IP geolocation data, and string usage, we found more than 130 connected artifacts comprising 61 email-connected domains, four additional IP addresses, an IP-connected domain, and 67 string-connected domains.

***If you wish to perform a similar investigation or learn more about the products used in this research, please don't hesitate to [contact us](#).***



**Disclaimer:** We take a cautionary stance toward threat detection and aim to provide relevant information to help protect against potential dangers. Consequently, it is possible that some entities identified as “threats” or “malicious” may eventually be deemed harmless upon further investigation or changes in context. We strongly recommend conducting supplementary investigations to corroborate the information provided herein.

## Appendix: Sample Artifacts

### Sample Email-Connected Domains

- housekeeperschoice[.]com
- heattulsa[.]com
- realestateosage[.]com
- landosage[.]com
- flex-fuelautos[.]com
- isdadocs[.]info
- thepowerlevel[.]org
- cabieuse[.]com
- actu-buzzly[.]fr
- actu-minutenews[.]fr
- actu-closermag[.]fr
- actu-cosmopolitan[.]fr
- actu-reportagesphotos[.]fr
- actu-24matins[.]fr
- actu-20minutes[.]fr
- actu-medisite[.]fr
- actu-football365[.]fr
- photo-call[.]fr
- buzz-sportif[.]fr
- news-elle[.]fr

### Sample Additional IP Addresses

- 103[.]28[.]91[.]193
- 45[.]128[.]135[.]122

### Sample String-Connected Domains

- electricianintulsa[.]com
- electricianstulsanearme[.]com
- electriciantulsa[.]com
- electricaltulsaok[.]com
- electricians-tulsa[.]com
- electricianneartulsa[.]com
- electricalservicestulsa[.]com
- electriciantulsa[.]net
- electricianstulsa[.]com
- electriciantulsanearme[.]com
- electrician-tulsa[.]com
- electricaltulsanearme[.]com
- electricprotulsa[.]com
- electriciantulsaok[.]com
- electriccarstulsa[.]com
- electriciantulsaokla[.]com
- electricianstulsaok[.]com
- electricalcontractorstulsa[.]com
- electriciansintulsa[.]com
- electricianstulsaok[.]net



