



# Illuminating ShadyPanda DNS Infrastructure Facts

## Table of Contents

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

## Executive Report

Koi Security recently published a report on ShadyPanda, which launched a seven-year-long campaign said to have affected the browsers of 4.3 million Chrome and Edge users to date. How has the campaign lasted so long? Some of the actors' extensions were featured and verified by Google, resulting in instant trust and massive distribution. Over time, they weaponized browser marketplaces by building trust, accumulating users, and pushing malicious silent updates.

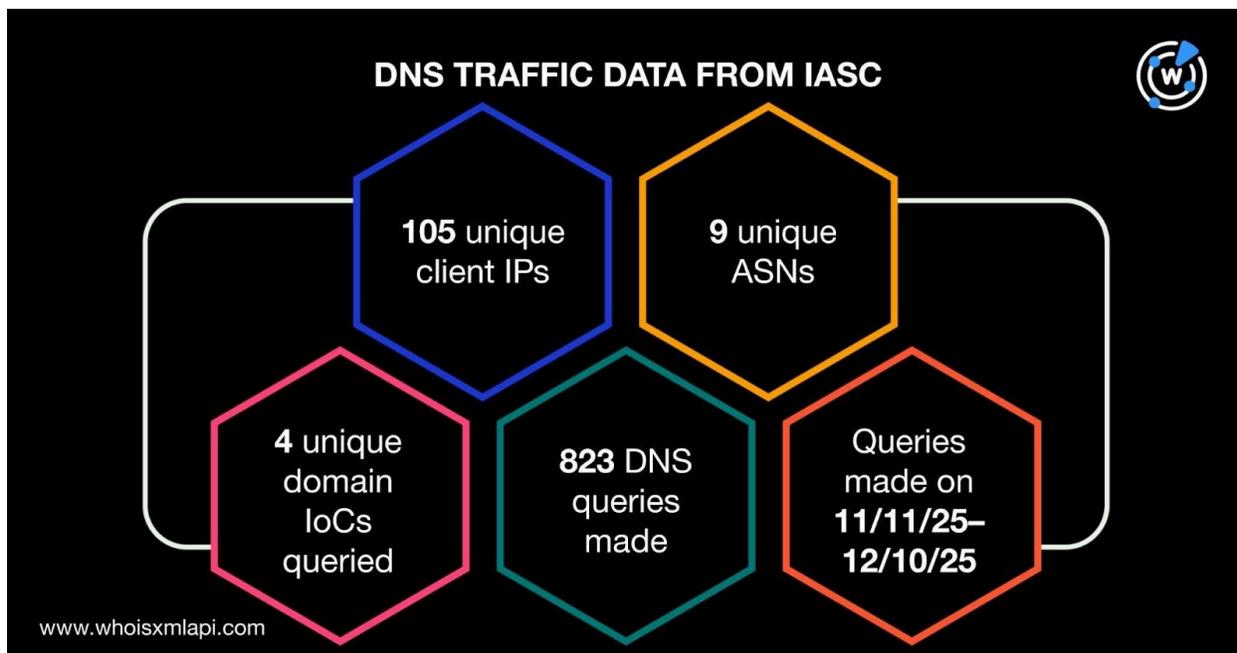
Koi identified [seven IoCs](#) comprising four domains and three subdomains. After extracting unique domains from the subdomains, we accumulated six domains and three subdomains for further analysis. Note that we queried the six domains on the [WhoisXML API MCP Server](#) and discovered that none of them were legitimate, making them worthy of further analysis.

Our in-depth investigation led to these discoveries:

- 105 unique client IP addresses communicated with four domains identified as IoCs
- 735 email-connected domains, one turned out to be malicious
- Seven IP addresses, six turned out to be malicious
- 18 IP-connected domains
- 76 string-connected domains

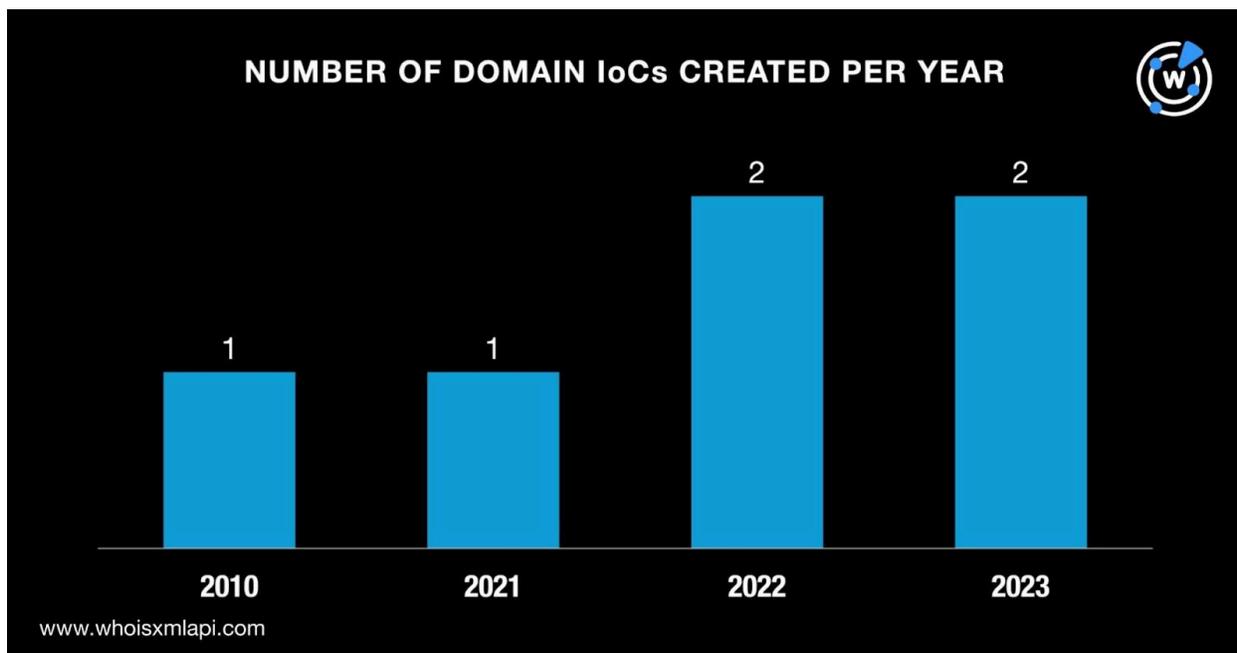
## The Hunt for More Information on the ShadyPanda IoCs

First, sample network traffic data from the [IASC](#) based on a total of 823 DNS queries showed that 105 unique client IP addresses under nine distinct ASNs communicated with four domains identified as IoCs between 11 November and 10 December 2025.



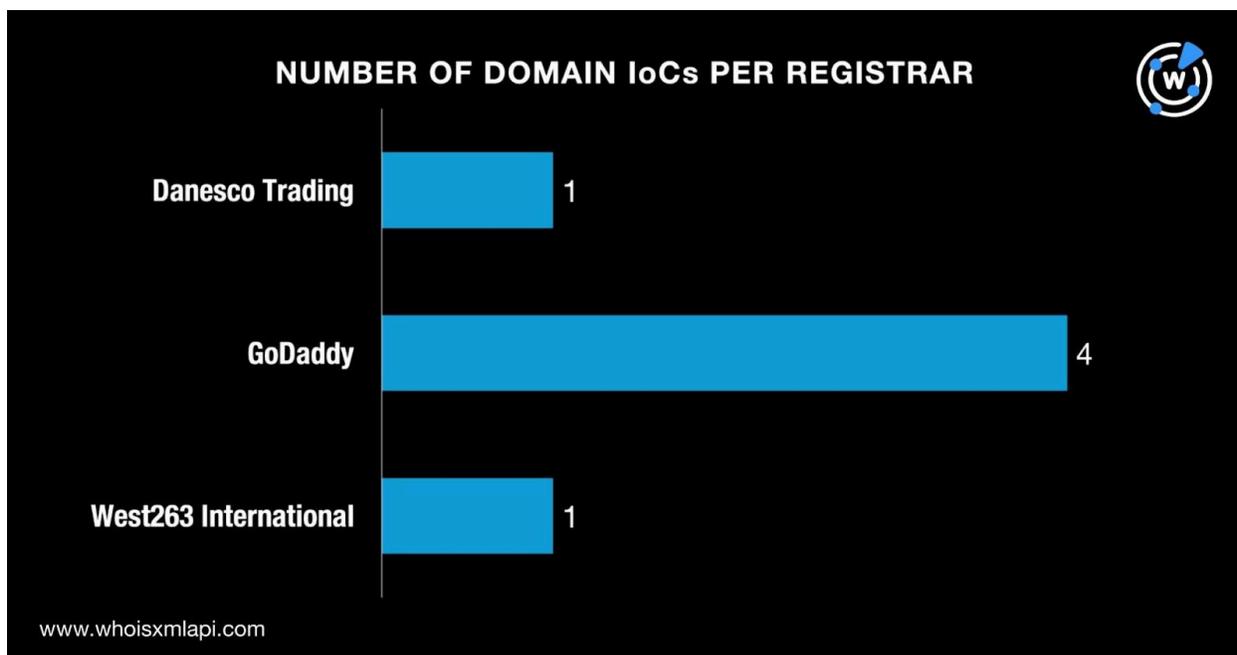
We then queried the six domains identified as IoCs on [WHOIS API](#) and discovered that:

- They were registered between 15 March 2010 and 7 September 2023. Two domains each were registered in 2022 and 2023 while one each were registered in 2010 and 2021.

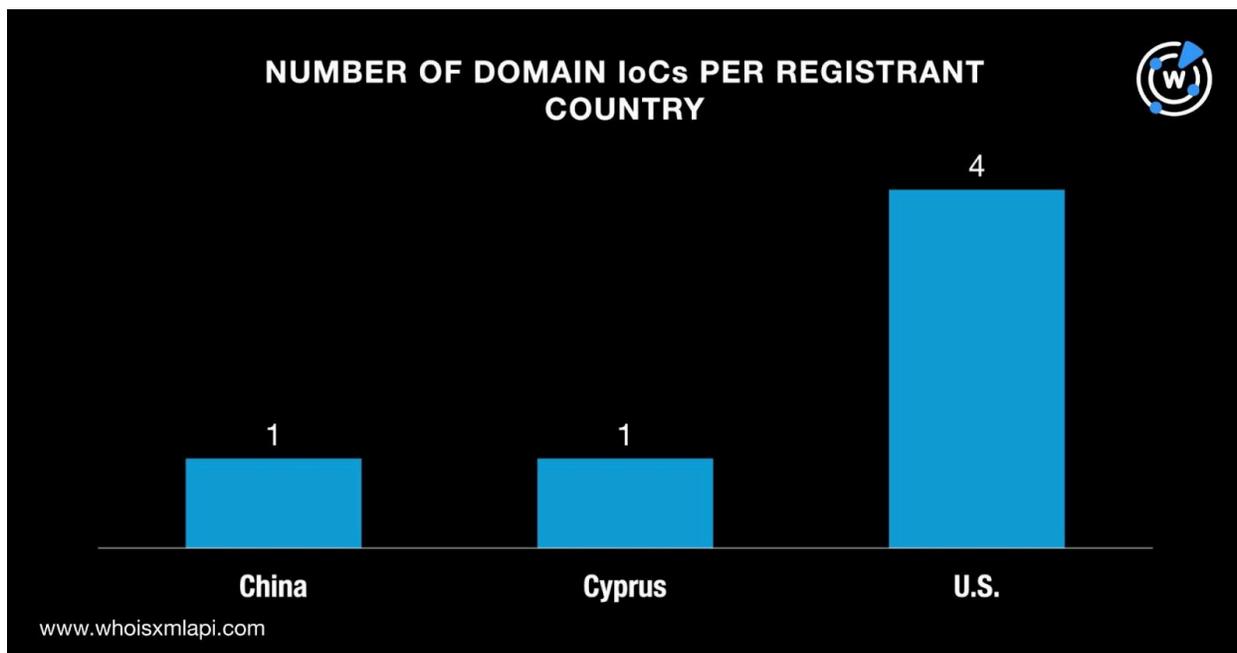




- They were administered by three registrars—four by GoDaddy and one each by Danesco Trading and West263 International.



- They were registered in three countries topped by the U.S., which accounted for four domains. One domain each, meanwhile, was registered in China and Cyprus.





A [DNS Chronicle API](#) query for the six domains identified as IoCs showed that all of them had 661 historical domain-to-IP resolutions over time. The domain gotocdn[.]com posted the earliest resolution date—26 May 2017. Take a look at more details for three examples below.

DOMAIN IoC	NUMBER OF RESOLUTIONS	RESOLUTION DATES
gotocdn[.]com	101	05/26/17–08/21/22
extensionplay[.]com	180	04/30/21–11/24/25
dergoodting[.]com	144	06/08/22–11/20/25

Next, we sought to uncover more insights regarding the three subdomains identified as IoCs and found out that:

- At first glance, api[.]cgatgpt[.]net could be typosquatting on ChatGPT’s popularity given that it contains a misspelled variant of the AI tool’s domain name. [Jake AI](#) revealed that it is relatively newly registered and privately registered. It was also set to expire within three years.



Of course! Here is what I found about the domain `api.cgatgpt.net` :

**WHOIS Information:**

- The domain `cgatgpt.net` was registered on September 7, 2023, and is set to expire on September 7, 2027.
- The owner's information is private, registered through "Domains By Proxy, LLC."
- The domain uses Cloudflare nameservers ( `kay.ns.cloudflare.com` and `walt.ns.cloudflare.com` ).

**DNS Information:**

- The subdomain `api.cgatgpt.net` points to the IP addresses `104.21.62.217` and `172.67.139.151` , which are part of Cloudflare's network.

**Threat Intelligence:**

- The domain `api.cgatgpt.net` is not currently flagged in our threat intelligence data.

In summary, `api.cgatgpt.net` is a relatively new domain with private ownership, hosted behind Cloudflare's network, and it does not have any current threat intelligence flags.

Would you like me to do a reverse IP search to see what other domains are hosted on the same IP addresses?

- While the root domain of `s-82923[.]gotocdn[.]com` and `s-85283[.]gotocdn[.]com` has been around for some time, it is privately registered. The two subdomains are now inactive.



Of course! Here is what I found about the domain `s-82923.gotocdn.com` :

**WHOIS Information:**

- The root domain `gotocdn.com` was registered on March 15, 2010, and is set to expire on March 15, 2028.
- The registrant's information is private and the country of registration is China.
- The domain uses the nameservers `ns1.myhostadmin.net` and `ns2.myhostadmin.net` .

**DNS Information:**

- The subdomain `s-82923.gotocdn.com` does not have any direct A records. This could mean it's used for internal purposes, is no longer active, or is part of a CNAME chain which is common for CDNs.

**Threat Intelligence:**

- The domain `s-82923.gotocdn.com` is not currently flagged in our threat intelligence data.

In summary, `s-82923.gotocdn.com` appears to be a subdomain related to a Content Delivery Network (CDN). The root domain `gotocdn.com` has a very long history, suggesting it's a legitimate service. The lack of a direct IP address for the subdomain and the "cdn" in the name are strong indicators of its role in a CDN.

Of course! Here is what I found about the domain `s-85283.gotocdn.com` :

**WHOIS Information:**

- The root domain `gotocdn.com` was registered on March 15, 2010, and is set to expire on March 15, 2028. This long history suggests it's an established service.
- The registrant's information is private, and the country of registration is China.
- The domain uses the nameservers `ns1.myhostadmin.net` and `ns2.myhostadmin.net` .

**DNS Information:**

- The subdomain `s-85283.gotocdn.com` does not have any direct A records. This often means it's used for internal purposes within a Content Delivery Network (CDN), is no longer in active use, or its resolution is handled through other DNS record types like CNAMEs.

**Threat Intelligence:**

- The domain `s-85283.gotocdn.com` is not currently flagged in our threat intelligence data, meaning it is not associated with any known malicious activity.

In summary, `s-85283.gotocdn.com` is a subdomain of a long-standing CDN provider, `gotocdn.com` , which is registered in China. The subdomain does not resolve to a direct IP address and has no security threats associated with it. It is likely part of their content delivery infrastructure.



## The Search for New ShadyPanda Artifacts

We began our search for new artifacts by querying the six domains identified as IoCs on [WHOIS History API](#) and discovered that three had email addresses in their historical WHOIS records. They had seven unique email addresses, in fact, and two were public addresses.

While the results of our [Reverse WHOIS API](#) query for the two public email addresses revealed that none appeared in current WHOIS records, both did show up in historical records. This step led to the discovery of 735 email-connected domains after those already identified as IoCs were filtered out.

A [Threat Intelligence API](#) query for the 735 email-connected domains showed that one has already been weaponized for phishing between 17 July and 2 December 2025 and generic threats between 18 July and 20 September 2025.

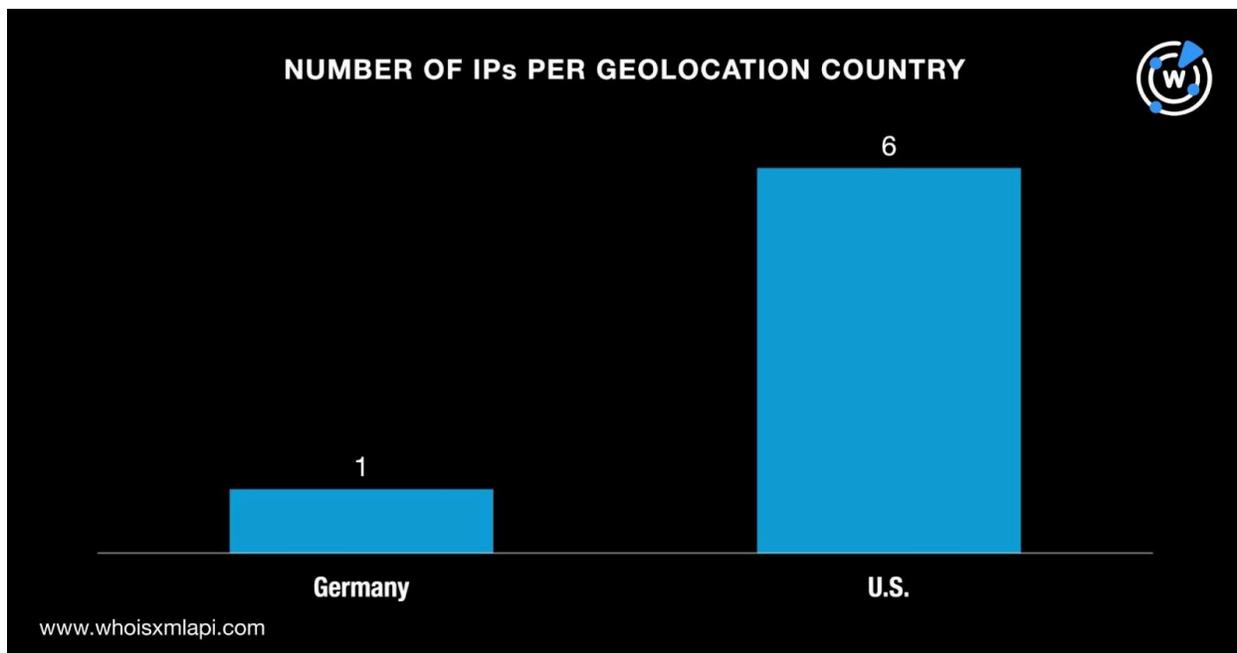
Next, we queried the six domains identified as IoCs on [DNS Lookup API](#) and found out that four had active IP resolutions. They resolved to seven unique IP addresses, in fact.

A Threat Intelligence API query for the seven IP addresses revealed that six have already figured in malicious campaigns. Take a look at more details for three examples below.

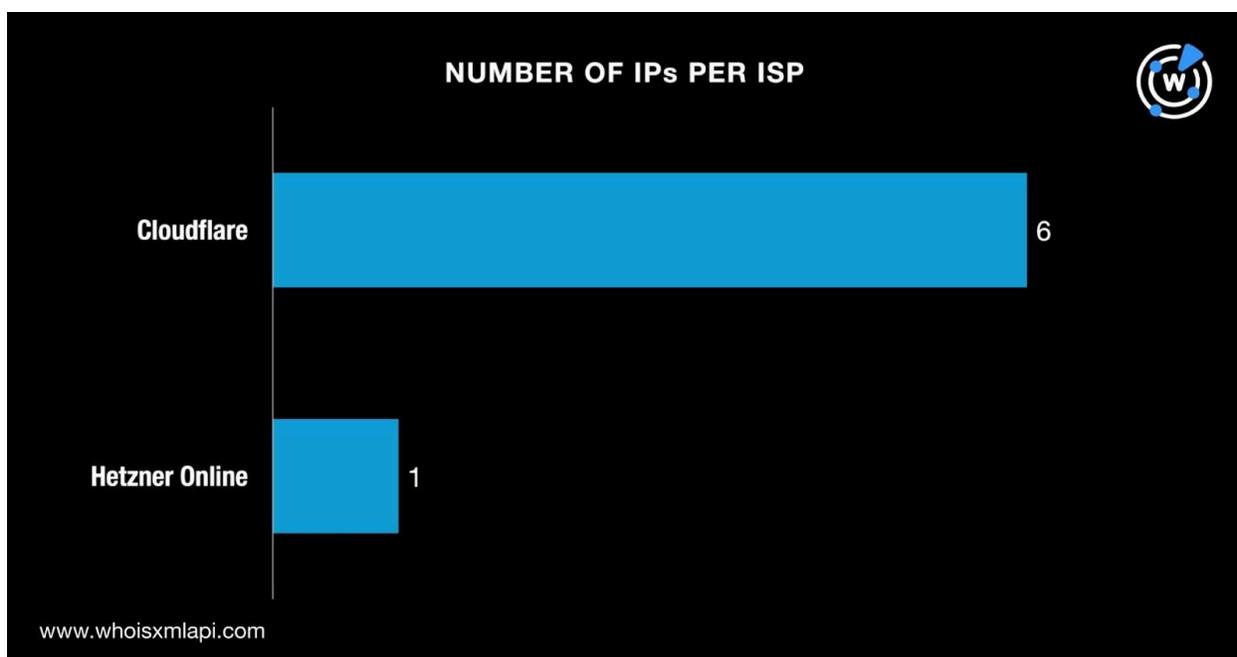
MALICIOUS IP ADDRESS	ASSOCIATED THREATS	DATES SEEN
104[.]21[.]45[.]44	Malware distribution	08/25/24–12/01/25
	Phishing	03/28/23–10/26/25
	Generic threat	03/29/23–10/06/25
104[.]21[.]49[.]170	Phishing	04/10/23–12/02/25
	Generic threat	03/30/23–12/01/25
	Malware distribution	02/12/24–09/30/25
104[.]21[.]74[.]14	Malware distribution	07/12/23–12/01/25
	Phishing	04/04/23–10/27/25
	Generic threat	04/03/23–10/04/25

To gather more information about the seven IP addresses, we queried them on [Bulk IP Geolocation Lookup](#) and discovered that:

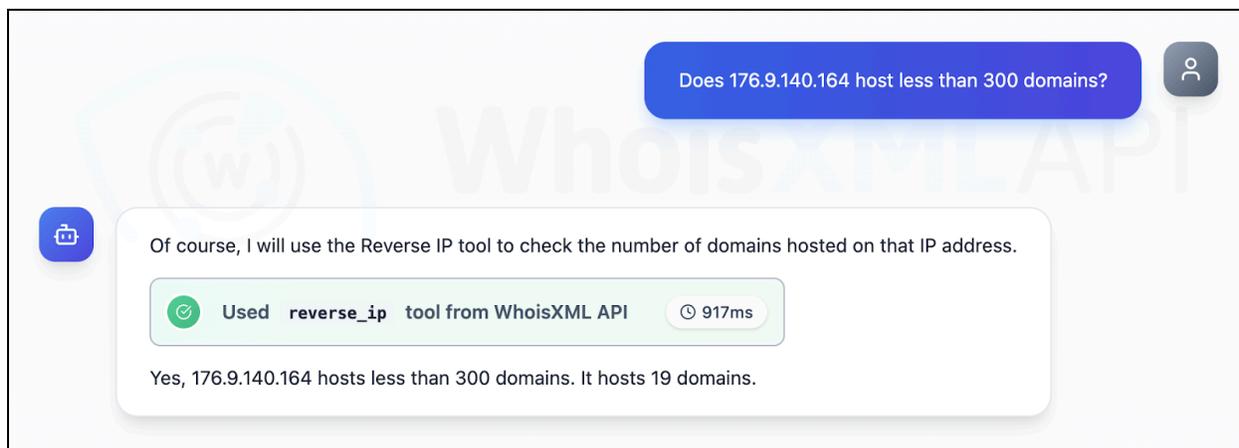
- They were geolocated in two countries—six in the U.S. and one in Germany.



- They were administered by two ISPs topped by Cloudflare, which accounted for six IP addresses. Hetzner Online, meanwhile, managed the remaining IP address.



Next, we sought to find out if any of the seven IP addresses could be dedicated hosts via Jake AI. We discovered that only one—176[.]9[.]140[.]164—was potentially dedicated.



It hosted 18 IP-connected domains after duplicates, those already identified as IoCs, and the email-connected domains were filtered out.

After that, we further scrutinized the six domains identified as IoCs and extracted the same number of unique text strings. [Domains & Subdomains Discovery](#) searches for them showed that three appeared in domains other than those already tagged as IoCs. In particular, we uncovered 76 string-connected domains that started with the strings **cgatgpt.**, **cleanmasters.**, and **gotocdn.** after duplicates, those already identified as IoCs, and the email- and IP-connected domains were filtered out.

—

Our in-depth investigation of the ShadyPanda attack allowed us to determine that 105 unique client IP addresses communicated with four domains identified as IoCs. It also led to the discovery of 836 new artifacts comprising 735 email-connected domains, seven IP addresses, 18 IP-connected domains, and 76 string-connected domains. It is also worth noting that seven of these artifacts have already been weaponized for cyber attacks.

***If you wish to 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

- 054[.]win
- 067[.]win
- 101-domainhosting[.]com
- accountexecutive[.]email
- addons[.]tv
- adstd[.]com
- backorderdomainer[.]com
- bankdn[.]com
- banketize[.]com
- camtld[.]com
- camtube[.]us
- canyaled[.]xn--vuq861b
- dai[.]top
- dailyws[.]com
- datingdn[.]com
- ebitcoinnetwork[.]com
- ebloggie[.]com
- edomainextension[.]com
- facebulletin[.]com
- faxingws[.]com
- federaltaxco[.]com
- galeazzi[.]email
- galeazzi[.]us
- gamblingws[.]com
- hkdns[.]hk
- hosting-sites[.]us
- hostmydomain[.]biz
- imagedn[.]com
- imagesdn[.]com
- incometaxes101[.]com
- jasminxxxx[.]com
- journaldomainer[.]com
- kf[.]win
- latestshow[.]com
- lawhelp101[.]com
- lawhelpnetwork[.]com
- manager[.]email
- marketdn[.]com
- marketsdomainer[.]com
- network-101[.]com
- networkdn[.]com
- networkdomainer[.]com
- onlinebloggie[.]com
- onlinetop[.]us
- paginate[.]com
- parkingdn[.]com
- parkingdomainer[.]com
- question101[.]com
- rbulletin[.]com
- registermydomain[.]net
- registrardn[.]com
- salesdn[.]com
- salestld[.]com
- salews[.]com
- taxesco[.]com
- taxescompany[.]com
- taxesws[.]com
- uchatting[.]com
- unifieddomainer[.]com
- unifieddomainnames[.]com
- videostld[.]com
- vwebcam[.]com
- webbloggie[.]com
- webcam[.]company
- webdebitcard[.]com
- xd[.]win
- xhamsters[.]xxx
- xiangxiangfamily[.]xn--vuq861b
- youtubes[.]xxx
- zoneads[.]com
- zoneadvertise[.]com



## Sample IP Addresses

- 104[.]21[.]45[.]44
- 104[.]21[.]49[.]170
- 104[.]21[.]74[.]14
- 172[.]67[.]148[.]3
- 172[.]67[.]152[.]177
- 172[.]67[.]209[.]176

## Sample IP-Connected Domains

- analytics[.]fdown[.]net
- docs-video[.]beta[.]datos[.]live
- docs[.]cz[.]beta[.]datos[.]live
- docs[.]exchange[.]beta[.]datos[.]live
- irc-docs[.]beta[.]datos[.]live
- ns0[.]credentials[.]beta[.]datos[.]live
- ns21[.]docs[.]beta[.]datos[.]live
- proxy1[.]docs[.]beta[.]datos[.]live
- safe[.]astian[.]org
- sip[.]credentials[.]beta[.]datos[.]live
- soft-credentials[.]beta[.]datos[.]live
- testcredentials[.]beta[.]datos[.]live

## Sample String-Connected Domains

- cgatgpt[.]cc
- cgatgpt[.]com
- cgatgpt[.]de
- cleanmasters[.]ae
- cleanmasters[.]at
- cleanmasters[.]be
- gotocdn[.]cn
- gotocdn[.]stream
- gotocdn[.]top