Following the VexTrio DNS Trail

Table of Contents

Executive Report

VexTrio, a traffic distribution system (TDS) provider believed to be an affiliate of ClearFake and SocGholish, among other threat actors, has been active since 2017. While many security researchers have studied ClearFake and SocGholish, VexTrio remained under the radar until Infoblox published their analysis, that is.

As it turned out, VexTrio has seemingly been in cahoots with ClearFake and SocGholish, among several other unknown threat actors or groups, providing them with the TDS they would need to carry out their specially crafted attacks.

Infoblox published an in-depth analysis of the VexTrio-aided campaigns and named 16 domains and seven subdomains as indicators of compromise (IoCs). They also mentioned the threat actors targeting TikTok and URL shortening services TinyURL, t.co, and is.gd. The WhoisXML API research team expanded the list of 23 domain IoCs in total (16 identified as IoCs and seven extracted from the subdomain IoCs) and found:

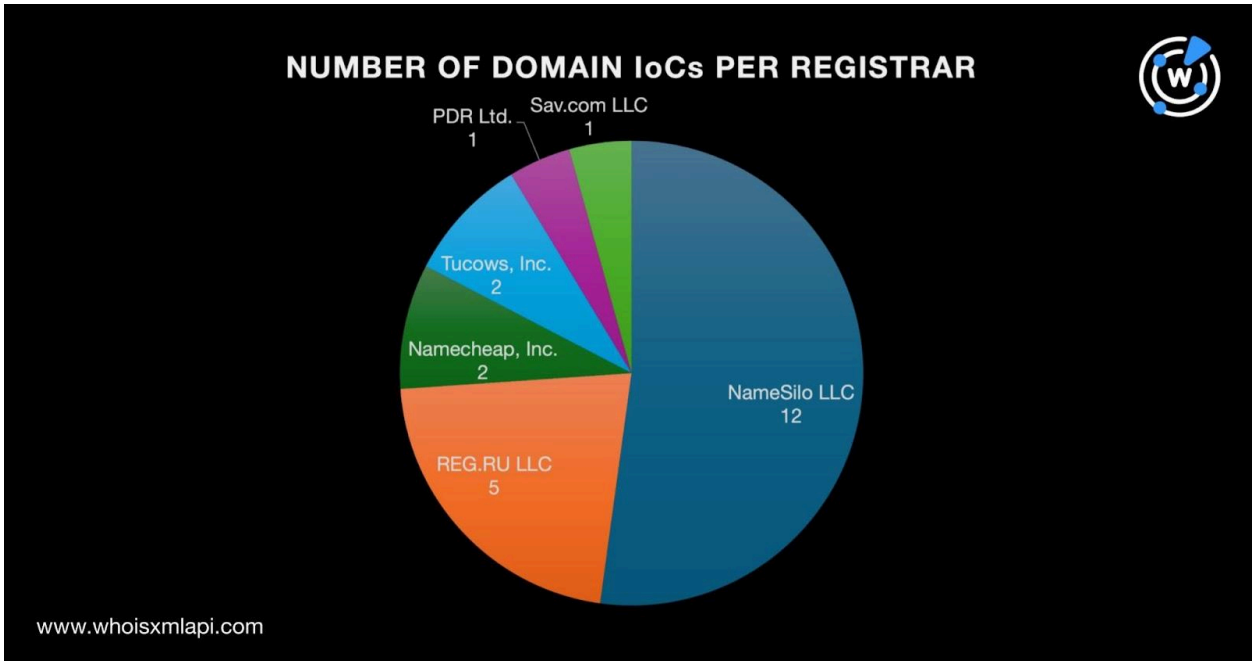
- 37 email-connected domains
- 13 IP addresses, 10 of which turned out to be malicious
- 207 IP-connected domains, 18 of which turned out to be malicious
- 247 string-connected domains

A sample of the additional artifacts obtained from our analysis is available for download from our website.

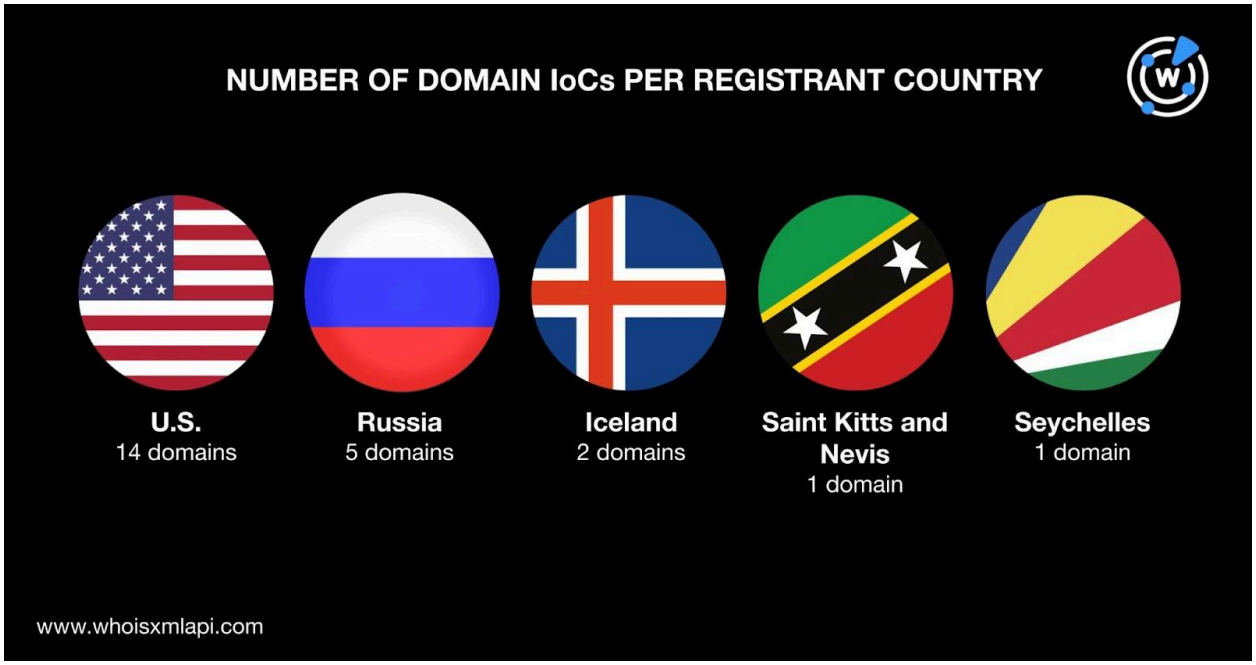
More on the VexTrio IoCs

We began our study with a bulk WHOIS lookup for the 23 domains identified as IoCs, which revealed that:

- They were administered by six registrars led by NameSilo LLC, which accounted for 12 domains. REG.RU LLC took the second spot with five domains. Namecheap, Inc. and Tucows, Inc. tied in third place with two domains each. PDR Ltd. and Sav.com LLC accounted for one domain each.



- A majority of them, 22 to be exact, were created in 2023 while one was created in 2021.
- They were registered in five countries led by the U.S., which accounted for 14 domains. Russia took second place with five domains. Iceland placed third with two domains. One domain each was registered in Saint Kitts and Nevis and Seychelles.



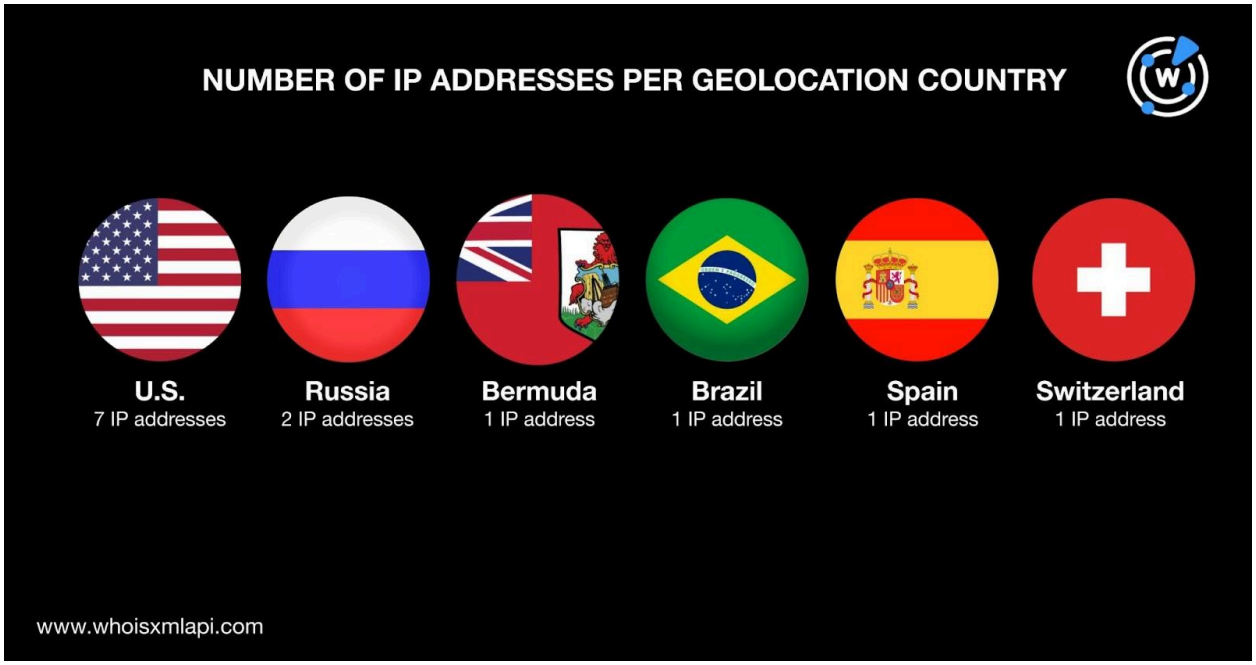
VexTrio IoC Connections

We began our analysis with WHOIS History API queries for the 23 domains identified as IoCs that led to the discovery of 19 email addresses from their historical WHOIS records after duplicates were removed. Seven of the email addresses were public.

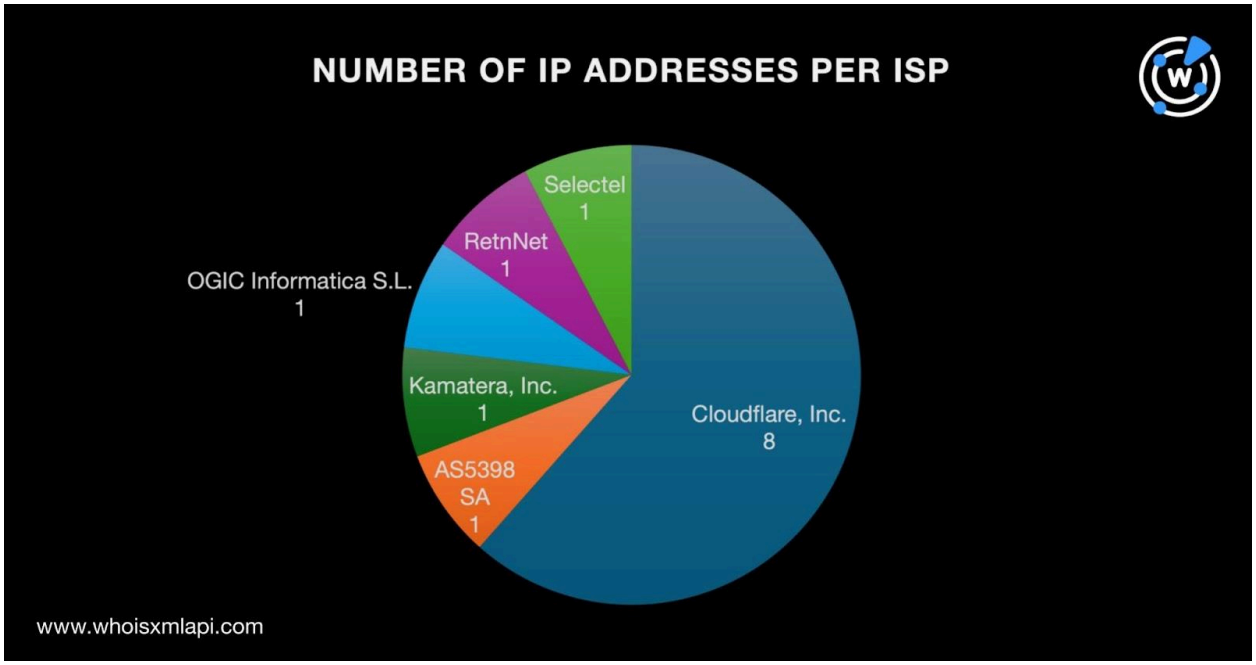
Reverse WHOIS API searches for the seven public email addresses provided us with 37 email-connected domains after filtering out duplicates and those already tagged as IoCs. Screenshot API revealed that only two remained accessible to date, both of which were up for sale.

Next, DNS lookups for the 23 domain IoCs showed they resolved to 13 unique IP addresses. IP geolocation lookups for them led to these findings:

- They were spread across six countries led by the U.S., which accounted for seven IP addresses. Russia followed with two IP addresses. Bermuda, Brazil, Spain, and Switzerland accounted for one IP address each.



- They were administered by six ISPs led by Cloudflare, Inc., which accounted for eight IP addresses. AS5398 SA; Kamatera, Inc.; OGIC Informatica S.L.; RetnNet; and Selectel accounted for one IP address each.



- Threat Intelligence API also revealed that 10 of the IP addresses were associated with various threats, including command and control (C2), generic threats, malware attacks, phishing, and suspicious activities. Take a look at detailed results for five of them below.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT TYPE
104[.]21[.]0[.]109	Generic Phishing
104[.]21[.]64[.]9	Generic Malware Phishing Suspicious
172[.]67[.]185[.]251	Generic Phishing
185[.]155[.]184[.]32	Malware
45[.]11[.]27[.]62	C2 Malware

Reverse IP lookups for the 13 IP addresses revealed that five of them could be dedicated. They also allowed us to gather 207 IP-connected domains after duplicates, the IoCs, and the email-connected domains were removed.

Threat Intelligence API showed that 18 of the IP-connected domains were associated with various threats, specifically command and control (C2) and malware attacks. Take a look at five examples below.

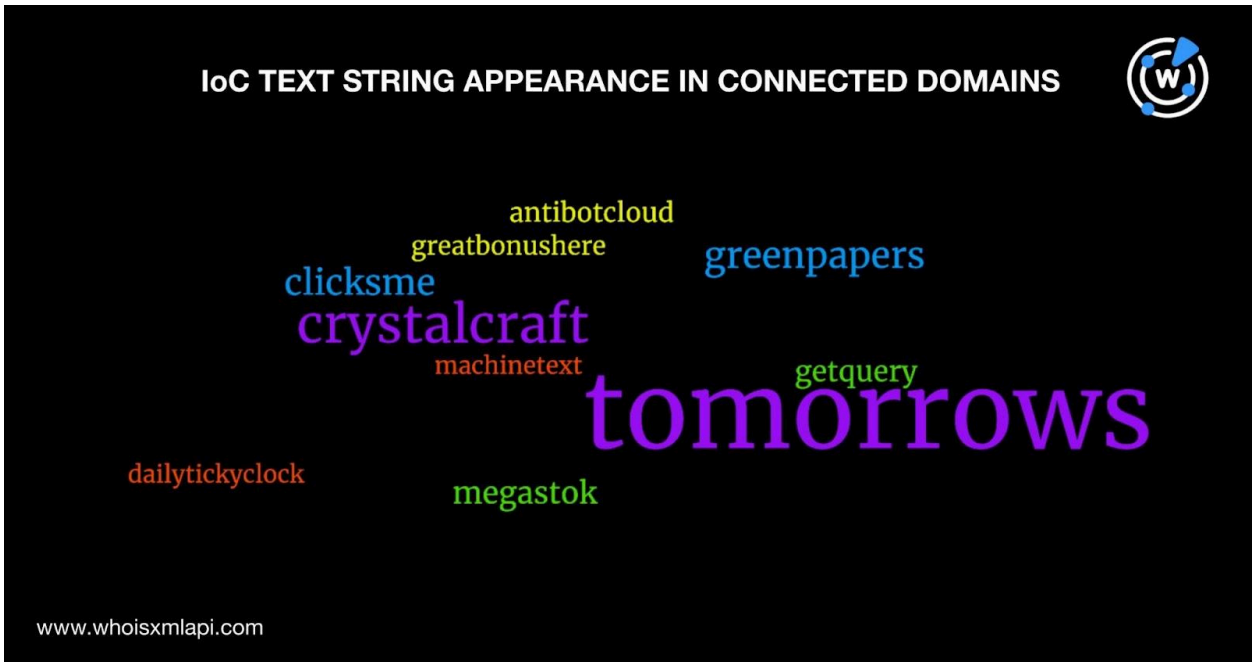
MALICIOUS IP-CONNECTED DOMAIN	ASSOCIATED THREAT TYPE
assistpayout[.]org	Malware
debasesingle[.]life	C2
jqueryns[.]com	C2 Malware
searchgear[.]pro	Malware
thewinjackpot[.]life	Malware

Screenshot lookups for the 18 malicious IP-connected domains showed that all of them remained live despite 17 leading to error pages. One domain—jqueryns[.]com—was parked.

Next, we used Domains & Subdomains Discovery to search for domains that contained text strings that appeared among the domain IoCs. We uncovered 247 domains after filtering out duplicates, the IoCs, and the email- and IP-connected domains that started with these strings:

- **antibotcloud.**
- **clicksme.**
- **crystalcraft.**
- **dailytickyclock.**
- **getquery.**
- **greatbonushere.**
- **greenpapers.**
- **machinetext.**
- **megastok.**
- **tomorrows.**

The word cloud below shows a representation of the 247 string-connected domains' presence in the DNS.



Signs of Platform Impersonation for Other Campaigns

The Infoblox report mentioned VexTrio impersonating TikTok for their campaigns. Specifically, the threat actors seemingly created four subdomains containing the text string **tiktok.**, namely:

- tiktok[.]megastok[.]top
- tiktok[.]superbowsm[.]top
- tiktok[.]supersbows[.]us
- tiktok[.]tomorrows[.]top

We used Domains & Subdomains Discovery to look for similar subdomains created since 16 December 2023, around the time Infoblox said the campaign began. We found 25 **tiktok.**-containing subdomains, 18 of which remained accessible albeit mostly leading to error pages. They could have been used for testing and left dangling.

In addition, we searched for **tiktok.**-containing domains created within the same time frame and found six such web properties. Two continued to host live pages to date. WHOIS record comparisons with tiktok[.]com—the official TikTok domain—showed that none of them could be publicly attributed to the company using its registrant organization as reference.

—

Our VexTrio IoC expansion analysis led to the discovery of 504 connected web properties comprising 37 email-connected domains, 13 IP addresses, 207 IP-connected domains, and 247 string-connected domains. It also unveiled that 28 of these digital assets were malicious. On top of all that, we also identified 31 domains and subdomains containing **tiktok.** that could figure in other malicious campaigns if weaponized.

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

- appbar[.]xyz
- artbizcoach[.]org
- diaoman[.]xyz
- flexiblenetworks[.]org
- foodbizcoach[.]org
- healthbizcoach[.]org
- hiphoper[.]xyz
- huanba[.]xyz
- huangjindao[.]xyz
- ipwz[.]site
- jimu[.]date
- kaidu[.]xyz
- kangjiu[.]xyz
- luosuo[.]xyz
- microeurope[.]org
- musicbizcoach[.]org

- nearline[.]xyz
- nongba[.]xyz
- partnershops[.]org
- pianjia[.]xyz

Sample IP Addresses

- 104[.]21[.]0[.]109
- 104[.]21[.]2[.]50
- 104[.]21[.]40[.]248
- 104[.]21[.]64[.]9
- 172[.]67[.]128[.]183
- 172[.]67[.]158[.]143
- 172[.]67[.]173[.]188

Sample IP-Connected Domains

- 00-youtubie[.]xyz
- 0880ma[.]online
- 15-youtubie[.]xyz
- 31-youtubee[.]xyz
- 4ce58e2613[.]shop
- 798672f6b2[.]store
- addcoinbonus[.]life
- afforchink[.]top
- assistpayout[.]org
- benteyispa[.]com
- berretramos[.]com
- best-win-touch[.]life
- bestelightfuldates[.]life
- bestprizerhere[.]life
- bigbricks[.]org
- bigultimatebonus[.]life
- bigwinningzone[.]life
- blackzone[.]buzz
- bonusaward[.]life
- bonuswinprice[.]life
- bowreches[.]com
- bundchent[.]com
- caragocroc[.]com
- cardigurro[.]com
- caseyzem[.]top
- chaletmonix[.]com
- chentlopi[.]com
- chestedband[.]org
- chimpvero[.]top
- chuchavuali[.]com
- chupamelo[.]top
- clansssbs[.]sbs
- codecruncher[.]pro
- cointheprizes[.]life
- commerce[.]vsys[.]top
- confirmapply[.]org
- craigthomax[.]com
- crubotuni[.]com
- crulborestor[.]com
- cumberyey[.]com
- darkmansion[.]org
- debasesingle[.]life
- doblixamos[.]com
- doctorkiki[.]me
- drilledgas[.]org
- espendokrug[.]top
- expres-bonustop[.]life
- expres-newcash[.]life
- fayanturbo[.]com
- fellomisko[.]com

Sample String-Connected Domains

- antibotcloud[.]net
- antibotcloud[.]ru

- antibotcloud[.]store
- antibotcloud[.]su
- antibotcloud[.]xyz
- clicksme[.]biz
- clicksme[.]click
- clicksme[.]club
- clicksme[.]co[.]uk
- clicksme[.]com
- clicksme[.]cyou
- clicksme[.]ga
- clicksme[.]gq
- clicksme[.]icu
- clicksme[.]in
- clicksme[.]info
- clicksme[.]link
- clicksme[.]live
- clicksme[.]shop
- clicksme[.]site
- clicksme[.]top
- clicksme[.]us
- clicksme[.]world
- clicksme[.]xyz
- crystalcraft[.]ae
- crystalcraft[.]app
- crystalcraft[.]at
- crystalcraft[.]ca
- crystalcraft[.]cc
- crystalcraft[.]cf
- crystalcraft[.]cloud
- crystalcraft[.]club
- crystalcraft[.]cn
- crystalcraft[.]co
- crystalcraft[.]co[.]in
- crystalcraft[.]co[.]nz
- crystalcraft[.]co[.]uk
- crystalcraft[.]com
- crystalcraft[.]com[.]au
- crystalcraft[.]com[.]cn
- crystalcraft[.]com[.]pl
- crystalcraft[.]de
- crystalcraft[.]dk
- crystalcraft[.]eu
- crystalcraft[.]finance
- crystalcraft[.]fm
- crystalcraft[.]fr
- crystalcraft[.]fun
- crystalcraft[.]games
- crystalcraft[.]gq