Examining the DNS Underbelly of the Voldemort Campaign

Table of Contents

Executive Report

Toward the end of August 2024, a customized malware dubbed "Voldemort" based on strings found in its code was used in a cyber espionage campaign targeting various countries. The malicious code employed a relatively new mix of tools, tactics, and procedures (TTPs), including weaponized Google Sheets, government agency impersonation, and the presence of peculiar strings like "test" for filenames.

To date, the campaign is believed to have sent around 20,000 phishing emails impacting more than 70 organizations worldwide. Fellow security researchers have also identified 19 indicators of compromise (IoCs) comprising 10 subdomains and nine IP addresses.

To aid organizations with network protection, the WhoisXML API research team expanded the initial list of IoCs to identify more connected artifacts, namely:

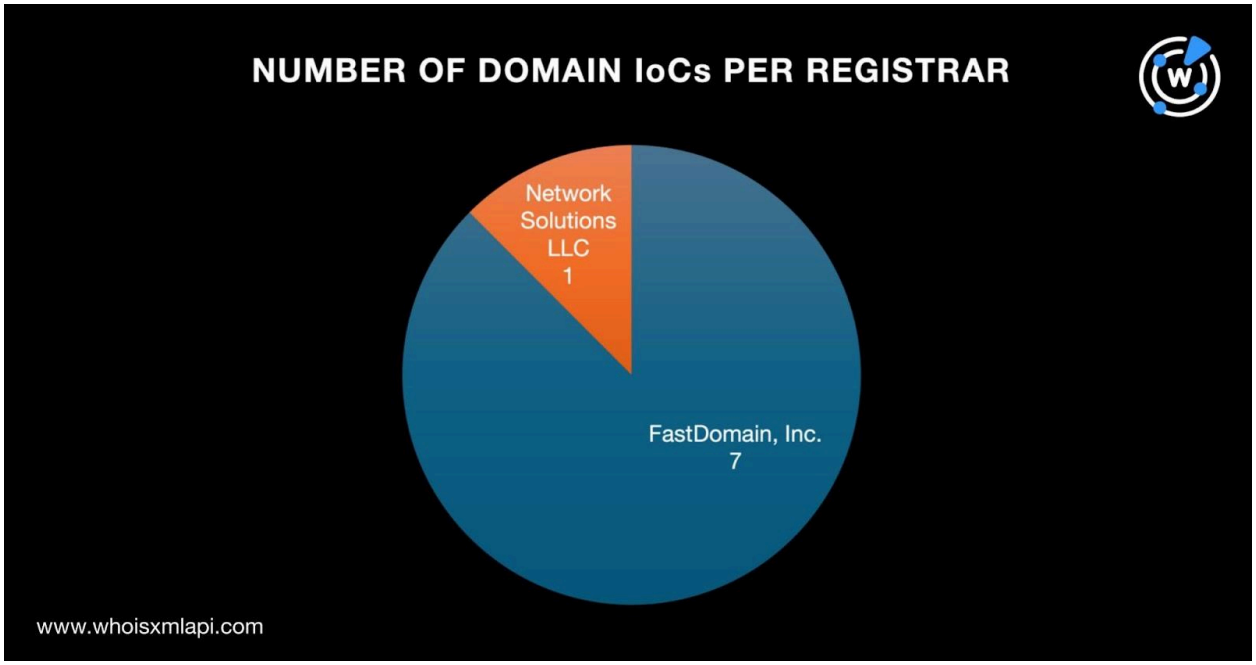
- 451 registrant-connected domains
- 298 email-connected domains
- Four additional IP addresses, all of which turned out to be malicious
- 28 string-connected domains
- 91 string-connected subdomains

A Closer Look at the Voldemort IoCs

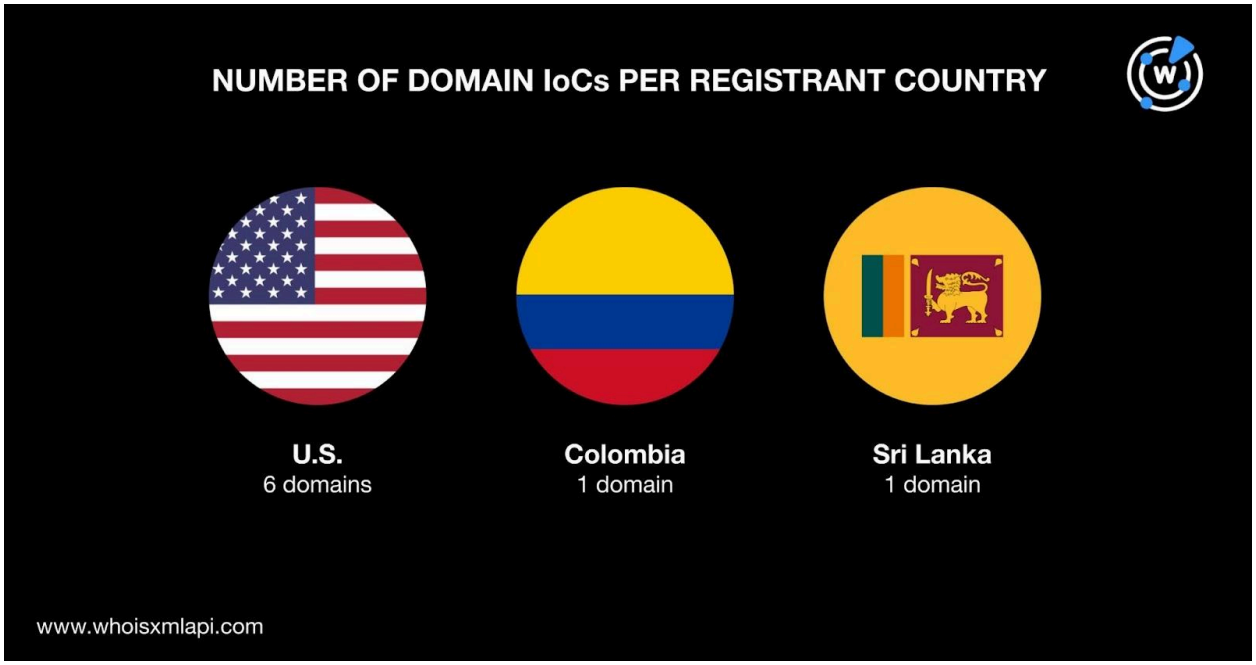
We began our analysis by looking for more information about the 19 IoCs.

To perform a bulk WHOIS lookup, we stripped the 10 subdomains down to the domain level, which provided us with nine domains for analysis. The lookup revealed that one domain name didn't have details in its current WHOIS record. We were thus left with eight domain IoCs for this step of the analysis.

- They were distributed between two registrars. Seven were administered by FastDomain, Inc. while one fell under the purview of Network Solutions LLC.



- All eight domain IoCs were created in 2023, most likely just for the campaign's use.
- They were spread across three registrant countries led by the U.S., which accounted for six domain IoCs. One domain each was registered in Colombia and Sri Lanka.



- Three of the eight domain IoCs had public registrant details, specifically:
    - **nitrocreditfix[.]com:** Registrant email address, name, and organization.
    - **torresemello[.]com:** Registrant email address and name.
    - **viouni[.]com:** Registrant email address and name.

We then performed a bulk IP geolocation lookup for the nine IP addresses and found that they were all geolocated in the U.S. and administered by Cloudflare.

Voldemort IoC Digital Footprints

We then proceeded to expand the initial IoC list starting with reverse WHOIS searches for the eight domain IoCs. We used the three registrant email addresses, three registrant names, and one registrant organization we found in the current WHOIS records of three of the domain IoCs as search terms. Our searches led to the discovery of 451 registrant-connected domains after duplicates and the IoCs were filtered out.

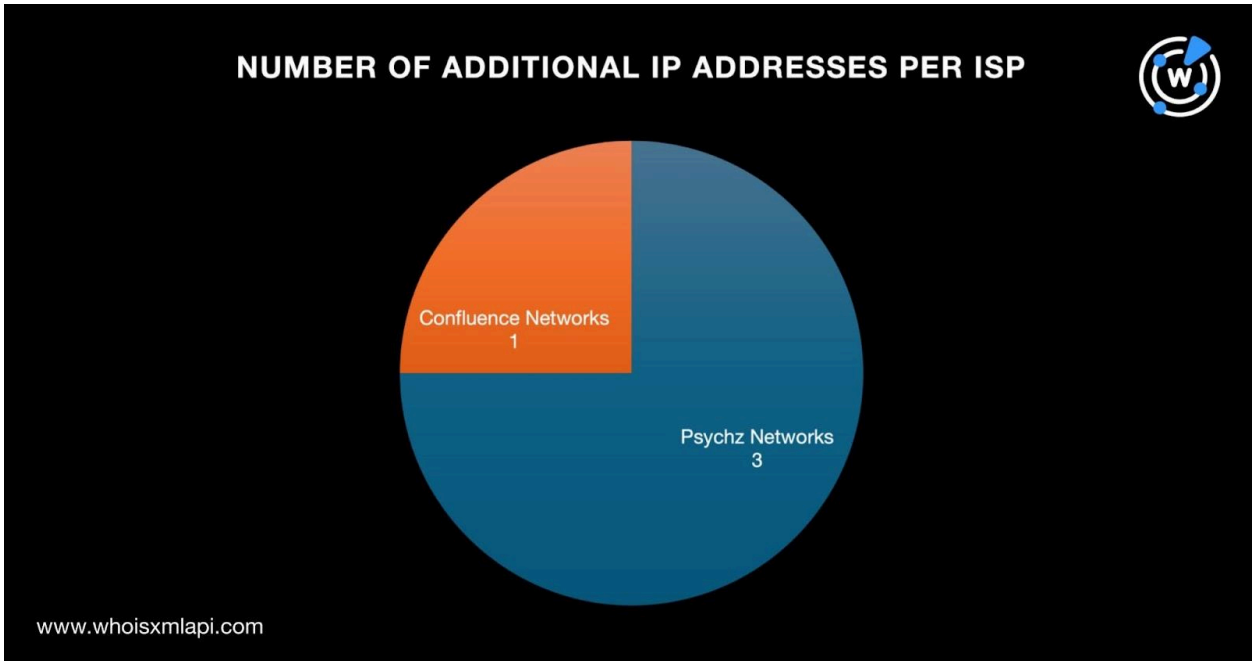
Next, we queried the eight domain IoCs on WHOIS History API and obtained 92 email addresses from their historical WHOIS records, 18 of which turned out to be public.

We queried the 18 public email addresses on Reverse WHOIS API. Thirteen of them were also found in the current WHOIS records of other domains. We uncovered 298 email-connected domains after filtering out duplicates, the IoCs, and the registrant-connected domains.

After that, we performed DNS lookups for the eight domain IoCs and discovered that five of them had active IP resolutions. Four of those IP addresses were not part of the initial IoC list. Threat Intelligence Lookup also showed that they were all associated with various threats. Take a look at two examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT TYPES
208[.]91[.]197[.]132	Attack Command and control (C&C) Generic Malware Phishing
66[.]81[.]203[.]133	Attack C&C Generic Malware Phishing Suspicious

A bulk IP geolocation lookup for the four additional IP addresses revealed that they were all geolocated in the U.S. They were split between two ISPs. Three IP addresses were administered by Psychz Networks and one by Confluence Networks.



We then ran reverse IP lookups for the 13 IP addresses we now have (i.e., nine IoCs and four additional) and found that they were all shared hosts, ending our search for IP-connected domains.

To cover all the bases, we scoured the DNS for domains and subdomains that started with the same text strings as the domain and subdomain IoCs via Domains & Subdomains Discovery. We uncovered 28 domains after removing duplicates, the IoCs, and the registrant- and email-connected domains. Like three of the domain IoCs, they began with three text strings, namely:

- **healthfloww**
- **shneez**
- **viouni**

We also found 91 subdomains after filtering out duplicates and the IoCs. Like five of the subdomain IoCs, they started with five text strings, namely:

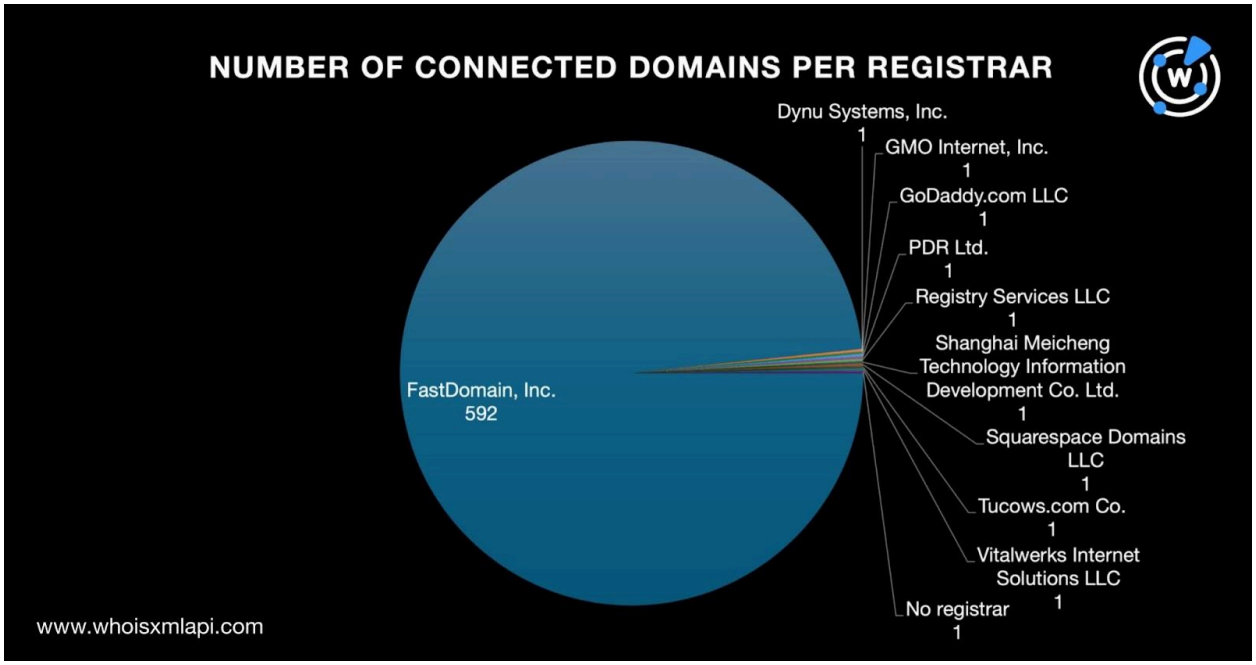
- **cluz.**
- **dryf.**
- **jzit.**
- **majc.**
- **urjaa.**

IoC-to-Artifact WHOIS Comparison

As the final step, we drew comparisons between the IoCs and the connected artifacts.

First, we dug up the WHOIS details of all the 777 connected domains and discovered that only 602 had current WHOIS records. We found that:

- A majority of them, 592 to be exact, were administered by FastDomain, Inc. Nine were distributed among nine other registrars, namely, Dynu Systems, Inc.; GMO Internet, Inc.; GoDaddy.com LLC; PDR Ltd.; Registry Services LLC; Shanghai Meicheng Technology Information Development Co. Ltd.; Squarespace Domains LLC; Tucows.com Co.; and Vitalwerks Internet Solutions LLC. One didn't have registrar details in its WHOIS record. Like 88% of the domain IoCs, 98% of the connected domains were managed by FastDomain, Inc.



- A huge chunk of the connected domains, 593 to be exact, were created in the same year as all of the domain IoCs were—2023. The nine remaining connected domains were created between 2010 and 2019.
- A majority of the connected domains, 580 to be exact, shared the domain IoCs' registrant countries—271 were registered in the U.S., 197 in Colombia, and 112 in Sri Lanka. Like 75% of the domain IoCs, 96% of the connected domains were registered in the U.S., Colombia, and Sri Lanka.

—

Our DNS deep dive into the 19 Voldemort IoCs led to the discovery of 872 connected artifacts comprising 451 registrant-connected domains, 298 email-connected domains, four IP addresses, 28 string-connected domains, and 91 string-connected subdomains. It's also interesting to note that all the additional IP addresses we found were malicious. WHOIS comparisons also showed that a majority of the connected domains shared the domain IoCs' details.

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 Registrant-Connected Domains

- 1ststeppingstones[.]com
- 2darlings[.]net
- 360-imagine[.]com
- 3rdstreetspalon[.]com
- 4acesliquidpackaging[.]com
- 4fcg[.]com
- abdullahsavas[.]net
- abpromotionsnow[.]com
- absolutescribe[.]com
- abubakersami[.]info
- academic-connections[.]com
- accom-herc[.]com
- aitkinquilts[.]com
- algorithmos[.]net
- antislamweapon[.]com
- aosug[.]org
- art2france[.]com
- asociacionipv[.]com
- atlosug[.]org
- autocatmonovar[.]com
- autodesguacespons[.]com
- autofaun[.]com
- bb-is[.]net
- bcmbg[.]com
- beachtrip[.]info
- beautiful-blooms[.]com
- beezmedio[.]com
- bekamaleona[.]com
- belezaris[.]com
- bellyrevelations[.]com
- benjamin-marcelis[.]com
- bestaia[.]com
- billhaycock[.]net
- blahdeblah[.]net
- blanjacod[.]com
- bostonuniversitycl[.]com
- bouquetent[.]com
- bugratekin[.]com
- buildcraft-urbanscape[.]com
- buildingconstructionpro[.]com
- cakesbyjoni[.]com
- camilledefago[.]com
- cankul[.]com
- celebratewithsanta[.]com
- century21gurrion[.]com
- cetattii[.]com
- cgearinc[.]com
- changethruchoice[.]com
- charles-studio[.]com
- charlieandcake[.]com

Sample Email-Connected Domains

- 000088[.]org
- 0070006[.]com
- 051100[.]live
- 0577001[.]com
- 106288[.]net
- 13066[.]mobi
- 23457890[.]com
- 2407788[.]com
- 277668[.]net
- 282811[.]net

- 2kdao[.]com
- 365dmconcepts[.]com
- 3765687[.]com
- 4roguz[.]com
- 4zhibo[.]apartments
- 517888[.]biz
- 5280lender[.]com
- 558551[.]net
- 6338888[.]net
- 63399888[.]com
- 656666[.]biz
- 67mi[.]net
- 75000[.]biz
- 781222[.]live
- 7878778[.]net
- 78906789[.]com
- 7915297[.]com
- 890123[.]net
- 9887997[.]com
- acicorp[.]net
- acta-llc[.]com
- adaikam[.]com
- advanceddataadministration[.]com
- affordablemedicalservices[.]net
- agioccc[.]us
- agw198[.]com
- alecalert[.]com
- alensen[.]com
- alessaeng[.]com
- altrolato[.]com
- americanarcologies[.]org
- amlo4tmx[.]com
- apartfashion-bg[.]com
- areejmarquee[.]com
- arenadirecto[.]com
- arielpenaililllo[.]com
- artenalinha[.]com
- atgdigitech[.]com
- aubergeleheron[.]net
- aurorajazzfest[.]com

Sample String-Connected Domains

- healthfloww[.]xyz
- healthflowwellness[.]ca
- healthflowwellness[.]com
- shneeze[.]mobi
- shneezenyc[.]com
- shneezgroup[.]com
- shneeztechnology[.]com
- shneeztransport[.]com
- viouni[.]fm
- viounic[.]club
- viounicsipu[.]tk
- viounicupassoeda[.]tk
- viouniesup[.]tk
- viounifati[.]tk

Sample String-Connected Subdomains

- cluz[.]a[.]run[.]app
- cluz[.]cloud-fr1[.]unispace[.]io
- cluz[.]cust[.]prod[.]thingdust[.]io
- cluz[.]cust[.]testing[.]thingdust[.]io
- cluz[.]demo[.]datacenter[.]fi
- cluz[.]denhaag[.]nl[.]eu[.]org
- cluz[.]eastasia[.]azurestaticapps[.]net
- cluz[.]eu-2[.]evennode[.]com
- cluz[.]fra1-de[.]cloudjiffy[.]net
- cluz[.]hb[.]cldmail[.]ru
- cluz[.]hiltontravelagents[.]web-7[.]hiltonbusinessonline[.]com
- cluz[.]jed[.]wafaicloud[.]com
- cluz[.]njs[.]jelastic[.]vps-host[.]net
- cluz[.]ocelot[.]mythic-beasts[.]com
- cluz[.]portal[.]contenedortres[.]top

- cluz[.]portal21[.]contenedortres[.]top
- cluz[.]rag-cloud[.]hosteur[.]com
- cluz[.]us[.]reclaim[.]cloud
- cluz[.]website[.]yandexcloud[.]net
- cluz[.]westus2[.]azurestaticapps[.]net
- cluz[.]www[.]static-fractal[.]web-11[.]hiltonbusinessonline[.]com
- cluz[.]yali[.]mythic-beasts[.]com
- dryf[.]appengine[.]flow[.]ch
- dryf[.]chemistry[.]manchester[.]ac[.]uk
- dryf[.]cust[.]dev[.]thingdust[.]io
- dryf[.]de[.]w3lookup[.]net
- dryf[.]eu[.]meteorapp[.]com
- dryf[.]eu[.]platform[.]sh
- dryf[.]fi[.]cloudplatform[.]fi
- dryf[.]git-pages[.]rit[.]edu
- dryf[.]j[.]layershift[.]co[.]uk
- dryf[.]jls-sto1[.]elastx[.]net
- dryf[.]la1-c1-ia6[.]salesforceliveagent[.]com
- dryf[.]london[.]cloudapps[.]digital
- dryf[.]njs[.]jelastic[.]vps-host[.]net
- dryf[.]ocelot[.]mythic-beasts[.]com
- dryf[.]uk[.]reclaim[.]cloud
- dryf[.]us[.]reclaim[.]cloud
- dryf[.]user[.]srcf[.]net
- dryf[.]westus2[.]azurestaticapps[.]net
- dryf[.]wiffvycn1ehyxwkreg1yvhym7bn[.]jevuf3krjjcrpo4vncg[.]5qoxwnvw3bulje49ilpm3aufufqqrtlwkc[.]81bgmf[.]qst8ca9mmuqp6ynfdtn9has3gn[.]shofha[.]online
- dryf[.]wjnddmesfo[.]obvcikyt0cbvnrhokncqt1agv7iyjjt[.]se9pbm3o[.]pmglcipovj1ncq[.]mta-sts[.]2[.]rp8uioivtyxiepwdd7mxlfga2syyyk[.]gdtmyo[.]shofha[.]online
- dryf[.]wmajkulmwktt6srk0e8yb15vepn[.]8kzbellircmdk[.]onfnkyeomxioa4p5blx4rqijgojrpnwh[.]qljbsmdjesrxl4wjeq8tsgiznrnoxze[.]sknoa5ivvcevax[.]23d2ef[.]shofha[.]online
- dryf[.]wmu4raqyk2lneqbbr7tp4tjol1fys[.]fsdq8li[.]ddqclwgzawetuhc7edhsuvlkxi9bbs[.]wdfb1evv8vk1hzqkhnmnk9wvmgyowoav[.]hwws4atd7eoqmim[.]wcps63bkddr0[.]shofha[.]online
- jzit[.]alp1[.]ae[.]flow[.]ch
- jzit[.]api[.]stdlib[.]com