A DNS Investigation of the 32 Doppelganger Websites Seized by the U.S. Government

Table of Contents

Executive Report

The U.S. Office of Public Affairs issued a statement on 4 September 2024 regarding the seizure of 32 websites that are believed to be part of the so-called “Doppelganger” campaign. According to the press release, Doppelganger could be a Russian-sponsored cyberpropaganda campaign designed to target the U.S. and other nations using fake news distributed through cybersquatting and other specially crafted domains.

While the statement did not disclose the seized domain names, we were able to get the complete list from The Hacker News. Upon closer examination, not all of the domains mimicked popular news sites the world over, some seem to have been specifically created to peddle disinformation. Take a look at the table below for more details.

SEIZED DOMAIN	MIMICKING	DESCRIPTION
50statesoflie[.]media		Fake news site
acrosstheline[.]press		Fake news site
artichoc[.]io		Fake news site
bild[.]work	bild[.]de	German tabloid
faz[.]ltd	faz[.]net	German newspaper
forward[.]pw	forward[.]com	U.S. Jewish news site
fox-news[.]in	foxnews[.]com	U.S. news channel site

fox-news[.]top	foxnews[.]com	U.S. news channel site
grenzezank[.]com		Fake news site
holylandherald[.]com		Fake news site
honeymoney[.]press		Fake news site
lemonde[.]ltd	lemonde[.]fr	French newspaper
leparisien[.]ltd	leparisien[.]fr	French newspaper
levinaigre[.]net		Fake news site
lexomnium[.]com		Fake news site
meisterurian[.]io		Fake news site
mypride[.]press		Fake news site
pravda-ua[.]com	pravda[.]com[.]ua	Ukrainian newspaper
rbk[.]media	rbc[.]ru	Russian media site
rrn[.]media		Fake news site
shadowwatch[.]us		Fake news site
spiegel[.]agency	spiegel[.]de	German news site
sueddeutsche[.]co	sueddeutsche[.]de	German newspaper
tagesspiegel[.]co	tagesspiegel[.]de	German newspaper
tribunalukraine[.]info		Fake news site
truthgate[.]us	truthgate[.]so	Blog
ukrlm[.]info	ukrlm[.]so	Blog

uschina[.]online	uschina[.]org	Nonprofit organization site
vip-news[.]org		Fake news site
warfareinsider[.]us		Fake news site
waronfakes[.]com		Fake news site
washingtonpost[.]pm	washingtonpost[.]com	U.S. newspaper

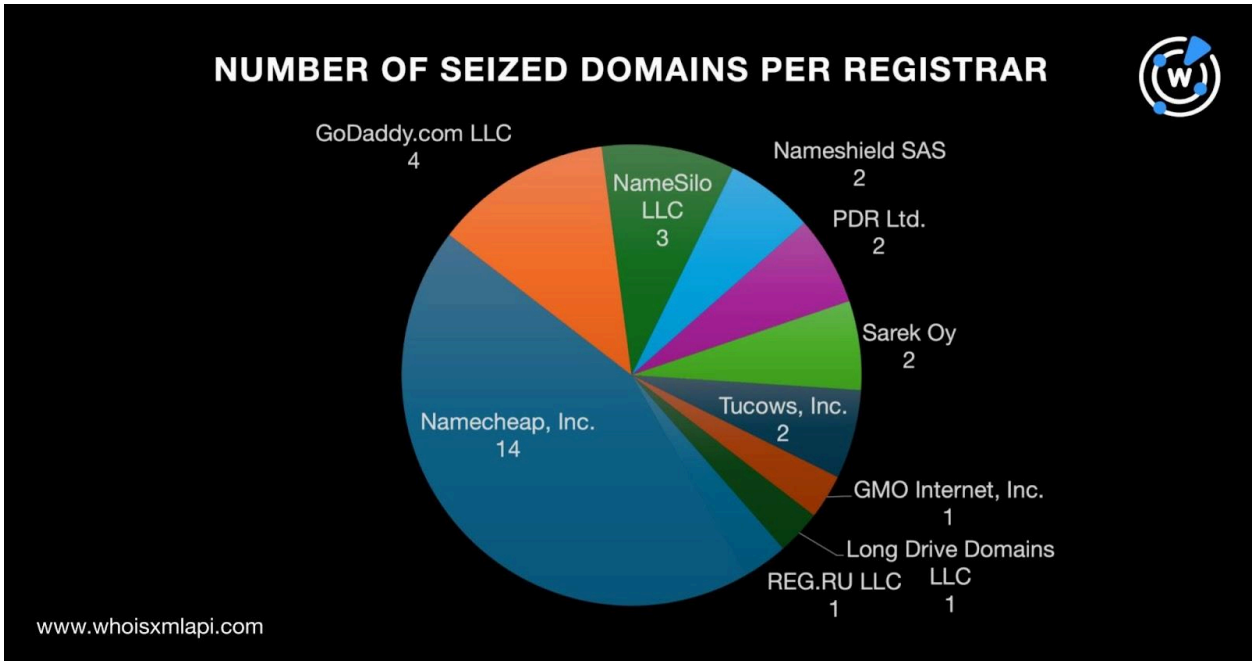
In fact, our online searches revealed that only half of the seized domains were seemingly cybersquatting on legitimate news or information sources. Nevertheless, we performed an expansion analysis for the 32 domain names to identify other connected artifacts. Our DNS deep dive led to the discovery of:

- 384 registrant-connected domains
- 123 email-connected domains
- 64 IP addresses, 54 of which turned out to be malicious
- 2,463 string-connected domains, six of which turned out to be associated with various threats

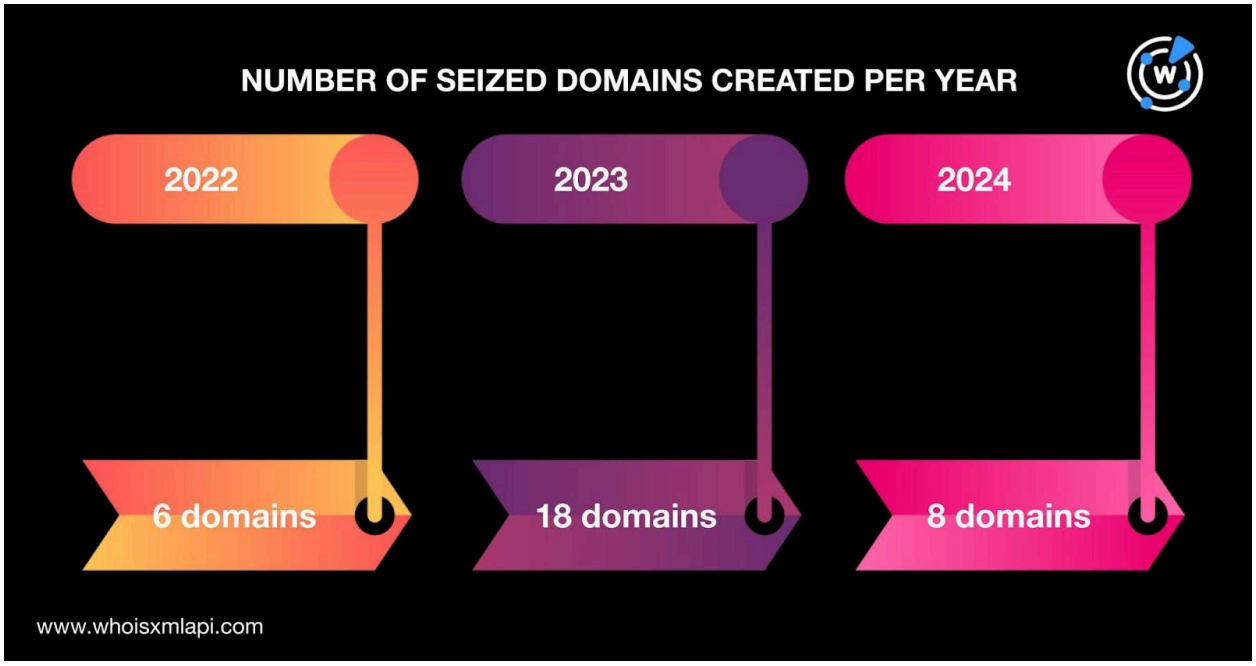
Facts about the Doppelganger Domains

We began our analysis by performing a bulk WHOIS lookup for the 32 domains, which showed that:

- Five domains had public registrant details. The domains lemonde[.]ltd and leparisien[.]ltd had public registrant organizations while shadowwatch[.]us, truthgate[.]us, and warfareinsider[.]us had public registrant email addresses and names.
- The domains were split among 10 registrars led by Namecheap, Inc. with 14 domains. GoDaddy.com LLC took the second spot with four domains. NameSilo LLC accounted for three domains while Nameshield SAS; PDR Ltd.; Sarek Oy; and Tucows, Inc. administered two domains each. The three remaining domains were administered by GMO Internet, Inc.; Long Drive Domains LLC; and REG.RU LLC.

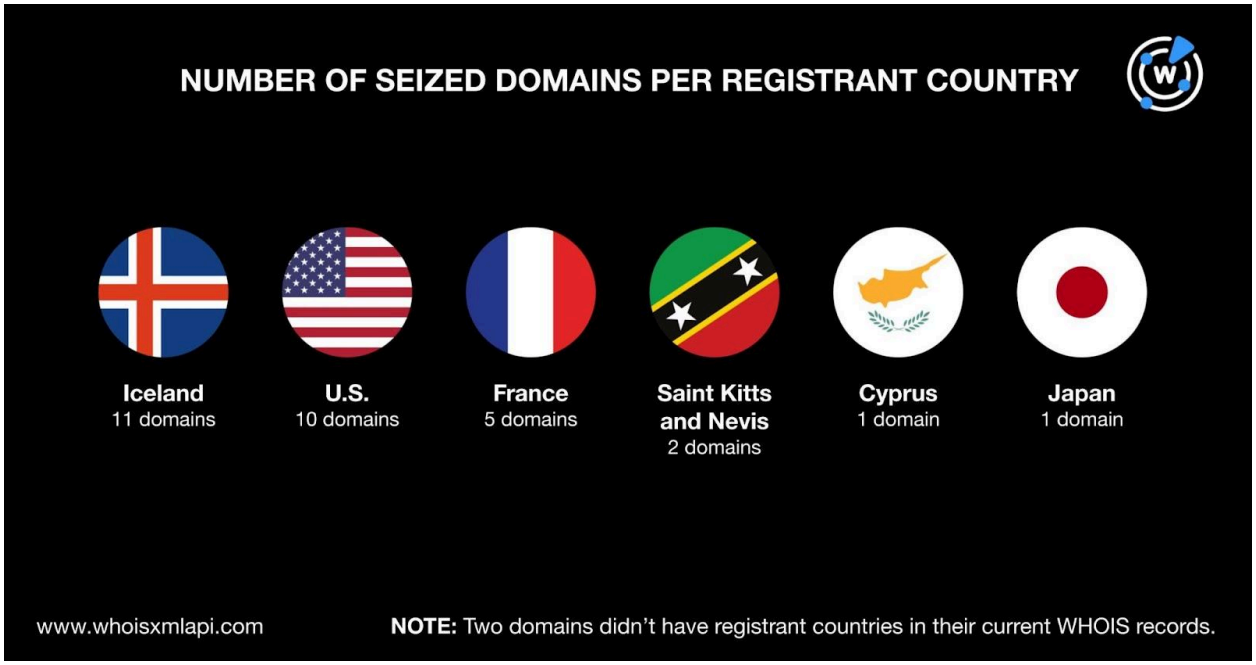


- The seized domains were created between 2022 and 2024. Six were specifically created in 2022, 18 in 2023, and eight in 2024.



- Thirty of the 32 domains were registered in six different countries topped by Iceland with 11 domains. The U.S. took second place with 10 domains while France came in third with five domains. Saint Kitts and Nevis accounted for two domains while Cyprus

and Japan had one domain each. Note that two domains did not have registrant countries in their current WHOIS records.



The Hunt for Doppelganger-Connected Web Properties

To find other web properties that could have ties to the Doppelganger disinformation campaign, we performed reverse WHOIS searches using the registrant information we obtained from our bulk WHOIS lookup earlier. We found 384 registrant-connected domains after filtering out duplicates and the seized domains.

Next, we queried the 32 seized domains on WHOIS History API, which led to the discovery of 30 email addresses in their historical WHOIS records. Eleven of those email addresses were public.

We queried the 11 public email addresses on Reverse WHOIS API, which allowed us to uncover 123 email-connected domains after duplicates, the seized domains, and the registrant-connected domains identified in the prior step were filtered out.

After that, we performed DNS lookups on the 32 seized domains and found that they resolved to 64 unique IP addresses.

When queried on Threat Intelligence API, 54 of the 64 IP addresses turned out to be associated with various threats. Take a look at five examples below.

MALICIOUS IP ADDRESS	ASSOCIATED THREAT TYPES
172[.]67[.]191[.]9	Generic Phishing
104[.]21[.]53[.]189	Malware Phishing Suspicious
172[.]67[.]176[.]235	Attack
172[.]67[.]199[.]6	Malware Attack Phishing Generic
104[.]21[.]31[.]110	Malware Command and control (C&C)

A bulk IP geolocation lookup for the 64 IP addresses revealed that they were all geolocated in the U.S. and administered by Cloudflare.

Next, we performed reverse IP lookups for the 64 IP addresses and found that they were all shared hosts, making it difficult to confidently identify associated IP-connected domains.

As our final step, we used Domains & Subdomains Discovery to search for domains that started with the same text strings as the seized domains. Thirty of the 32 strings from the seized domains provided results. We uncovered 2,463 string-connected domains that began with these strings:

- **50statesoflie.**
- **acrosstheline.**
- **artichoc.**
- **bild.**
- **faz.**
- **forward.**
- **fox-news.**
- **grenzezank.**
- **holylandherald.**
- **honeymoney.**
- **lemonde.**
- **leparisien.**
- **levinaigre.**
- **lexomnium.**
- **meisterurian.**
- **mypride.**
- **pravda-ua.**
- **rbk.**

- **rrn.**
- **shadowwatch.**
- **spiegel.**
- **sueddeutsche.**
- **tagesspiegel.**
- **truthgate.**
- **uschina.**
- **vip-news.**
- **warfareinsider.**
- **waronfakes.**
- **washingtonpost.**

Threat Intelligence API revealed that six of the string-connected domains were already tagged as malicious. Take a look at three examples below.

MALICIOUS STRING-CONNECTED DOMAIN	ASSOCIATED THREAT TYPES
honeymoney[.]su	Malware
washingtonpost[.]asia	Attack
washingtonpost[.]careers	Attack

Given that 16 of the seized domains could be cybersquatting on popular news sites, we sought to determine how many of the string-connected domains with the legitimate brand names were publicly attributable to the news agencies or organizations, if any, using WHOIS information.

First off, though, we needed to find out which of the domains possibly being mimicked had public WHOIS record details. We focused this step in our analysis on three of the mimicked domains and their typosquatting variants—foxnews[.]com (i.e., foxnews[.]in and fox-news[.]top), uschina[.]org (i.e., uschina[.]online), and washingtonpost[.]com (i.e., washingtonpost[.]pm).

A total of 264 of the 2,463 string-connected domains contained these strings:

- **fox-news.**
- **uschina.**
- **washingtonpost.**

Only 34 of the branded connected domains, containing **fox-news.** and **washingtonpost.**, could be publicly attributed to the U.S. news publishers. No branded connected domain was found containing **uschina.** that could be attributed to the legitimate organization.

—

Our investigation of the Doppelganger campaign unveiled 3,034 connected artifacts comprising 384 registrant-connected domains, 123 email-connected domains, 64 IP addresses, and 2,463 string-connected domains. Interestingly, 60 of these connected web properties may have already figured in 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 Registrant-Connected Domains

- 1emonde[.]fr
- abolemonde[.]fr
- abonnementlemonde[.]fr
- abonnementslemonde[.]fr
- aboslemonde[.]fr
- alert24[.]fr
- alerte24[.]fr
- art-interactif[.]com
- art-interactif[.]net
- art-interactif[.]org
- artinteractif[.]com
- artinteractif[.]net
- artinteractif[.]org
- arts-interactif[.]com
- arts-interactif[.]net
- arts-interactif[.]org
- arts-interactifs[.]com
- arts-interactifs[.]net
- arts-interactifs[.]org
- artsinteractifs[.]net
- artsinteractifs[.]org
- ateliers-lemonde[.]fr
- atlasducosmoslemonde[.]fr
- aujourdhui-en-france[.]app
- aujourdhui-en-france[.]biz
- aujourdhui-en-france[.]com
- aujourdhui-en-france[.]digital
- aujourdhui-en-france[.]fr
- aujourdhui-en-france[.]info
- aujourdhui-en-france[.]media
- aujourdhui-en-france[.]net
- aujourdhui-en-france[.]news
- aujourdhui-en-france[.]online
- aujourdhui-en-france[.]org
- aujourdhui-en-france[.]paris
- aujourdhui-en-france[.]press
- aujourdhui-etudiant[.]com
- aujourdhui[.]biz
- aujourdhui[.]fr
- aujourdhui[.]info
- aujourdhui[.]mobi
- aujourdhui[.]net
- aujourdhui[.]org
- aujourdhuienfrance[.]app

- aujourdhuienfrance[.]biz
- aujourdhuienfrance[.]com
- aujourdhuienfrance[.]digital
- aujourdhuienfrance[.]fr
- aujourdhuienfrance[.]info
- aujourdhuienfrance[.]media

Sample Email-Connected Domains

- 97bt[.]top
- allesgratis[.]click
- alpenland[.]news
- alpenland[.]space
- arbeit-ist-geil[.]com
- ballett[.]click
- ballett[.]rocks
- ballett[.]work
- ballettschule[.]link
- ballettschule[.]pro
- ballettschule[.]space
- barbeleg[.]com
- beleg[.]pro
- bewegung[.]space
- bodypainting[.]link
- buchung[.]jetzt
- catwalk[.]run
- childmodel[.]space
- clouddesign[.]click
- clouddesign[.]space
- clouddesign[.]work
- content-strategy[.]space
- creative-art[.]work
- darmann[.]technology
- echtsteil[.]net
- elfen[.]space
- energieausweis-steiermark[.]com
- erkunden[.]jetzt
- fashion-shooting[.]com
- fashiondesign[.]show
- feen[.]space
- filmmusic[.]space
- filmmusic[.]work
- filmmusik[.]pro
- filmmusik[.]space
- foto-strecke[.]com
- fotogirls[.]club
- fotojob[.]info
- fotokunst[.]pro
- fotomodel[.]love
- fotomodel[.]space
- fotomodel[.]video
- fotomodels[.]top
- fotoshooting[.]center
- fotoshooting[.]gratis
- fotoshooting[.]link
- fotoshooting[.]space
- fotostrecke[.]pro
- fotostudio[.]tokyo
- fototrail[.]net

Sample IP Addresses

- 104[.]21[.]38[.]70
- 172[.]67[.]191[.]9
- 172[.]67[.]146[.]198
- 104[.]21[.]53[.]189
- 172[.]67[.]169[.]176
- 104[.]21[.]12[.]247
- 172[.]67[.]176[.]235
- 104[.]21[.]32[.]183
- 172[.]67[.]199[.]181
- 104[.]21[.]71[.]157
- 172[.]67[.]184[.]231
- 104[.]21[.]51[.]76
- 172[.]67[.]223[.]251
- 104[.]21[.]0[.]251

- 172[.]67[.]181[.]212
- 172[.]67[.]199[.]6
- 172[.]67[.]192[.]40
- 104[.]21[.]59[.]98
- 172[.]67[.]147[.]160
- 104[.]21[.]31[.]110

Sample String-Connected Domains

- 50statesoflie[.]cc
- 50statesoflie[.]com
- 50statesoflie[.]so
- acrosstheline[.]au
- acrosstheline[.]blog
- acrosstheline[.]ca
- artichoc[.]be
- artichoc[.]cafe
- artichoc[.]cc
- bild[.]academy
- bild[.]adult
- bild[.]ae
- faz[.]adv[.]br
- faz[.]ae
- faz[.]aero
- forward[.]academy
- forward[.]ad[.]jp
- forward[.]adult
- fox-news[.]ai
- fox-news[.]biz
- fox-news[.]blog
- grenzezank[.]to
- holylandherald[.]online
- holylandherald[.]pw
- honeymoney[.]adult
- honeymoney[.]agency
- honeymoney[.]app
- lemonde[.]adult
- lemonde[.]ae
- lemonde[.]africa
- leparisien[.]ae
- leparisien[.]app
- leparisien[.]arab
- levinaigre[.]biz
- levinaigre[.]com
- levinaigre[.]so
- lexomnium[.]pw
- meisterurian[.]com
- meisterurian[.]to
- mypride[.]app
- mypride[.]asia
- mypride[.]biz
- pravda-ua[.]bond
- pravda-ua[.]cfd
- pravda-ua[.]click
- rbk[.]ac[.]th
- rbk[.]ae
- rbk[.]aero
- rrn[.]academy
- rrn[.]adv[.]br
- rrn[.]aero
- shadowwatch[.]co
- shadowwatch[.]com
- shadowwatch[.]de
- spiegel[.]ai
- spiegel[.]amsterdam
- spiegel[.]app
- sueddeutsche[.]app
- sueddeutsche[.]at
- sueddeutsche[.]bayern
- truthgate[.]com
- truthgate[.]info
- truthgate[.]io
- uschina[.]app
- uschina[.]biz
- uschina[.]business
- vip-news[.]at
- vip-news[.]biz

- vip-news[.]casino
- warfareinsider[.]cc
- warfareinsider[.]com
- waronfakes[.]cz
- washingtonpost[.]adult
- washingtonpost[.]agency
- washingtonpost[.]ai