WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

Searching for Potential Propaganda Vehicle Presence in the DNS

Table of Contents

Executive Report

The Citizen Lab recently uncovered an ongoing online propaganda campaign they have dubbed "PAPERWALL" that has been targeting local news outlets across 30 countries in Europe, Asia, and Latin America.

PAPERWALL bore similarities with HaiEnergy, an influence operation Mandiant reported about in July 2023. Both threats specifically drew significant portions of content from Times Newswire. But PAPERWALL seemed distinct in that it had different operators and unique tools, tactics, and procedures (TTPs).

The WhoisXML API research team dove deeper into the threat to uncover possible traces of PAPERWALL's presence in the DNS. We analyzed 132 indicators of compromise (IoCs) comprising 123 domain names and nine IP addresses, which led to the discovery of:

- 681 email-connected domains
- One additional IP address
- One IP-connected domain
- 193 string-connected domains, one of which turned out to be malicious

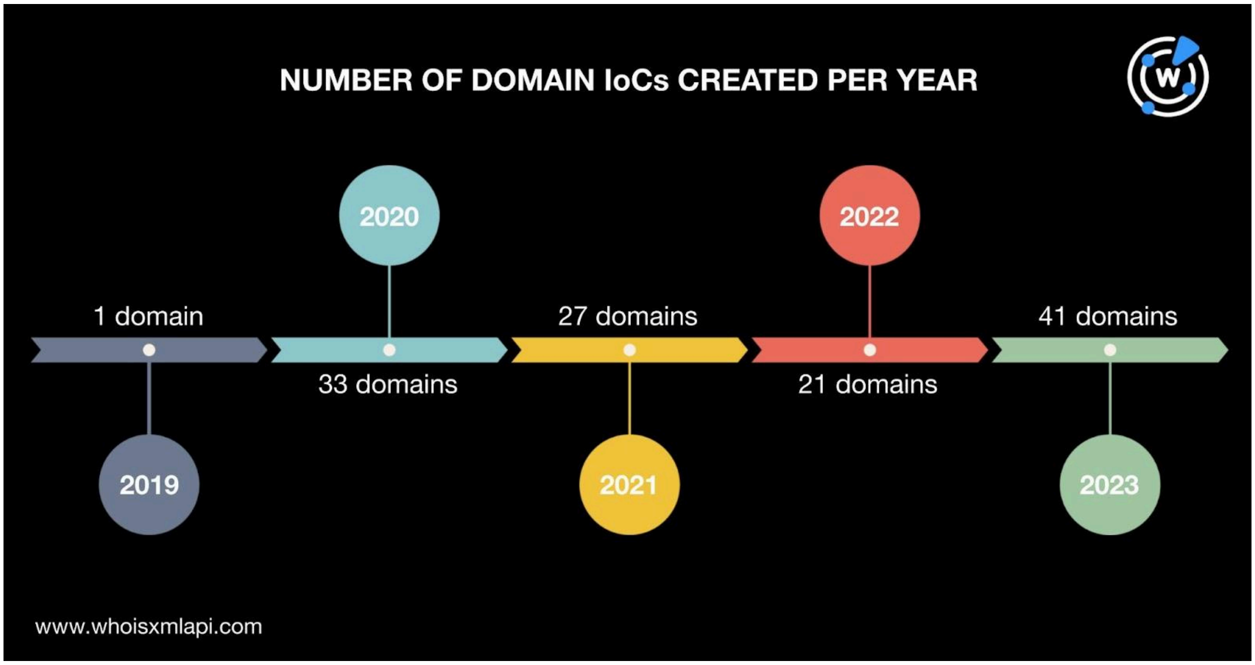
PAPERWALL IoC DNS Facts

As our usual first step, we sought to find more information about the 132 IoCs The Citizen Lab reported.

We started with a bulk WHOIS lookup for the 123 domain names identified as IoCs, which revealed that:

- All of them were obtained from GoDaddy.com LLC.

- They were created between 2019 and 2023. A majority, 41 to be exact, were created in 2023, 33 in 2020, 27 in 2021, 21 in 2022, and one in 2019.

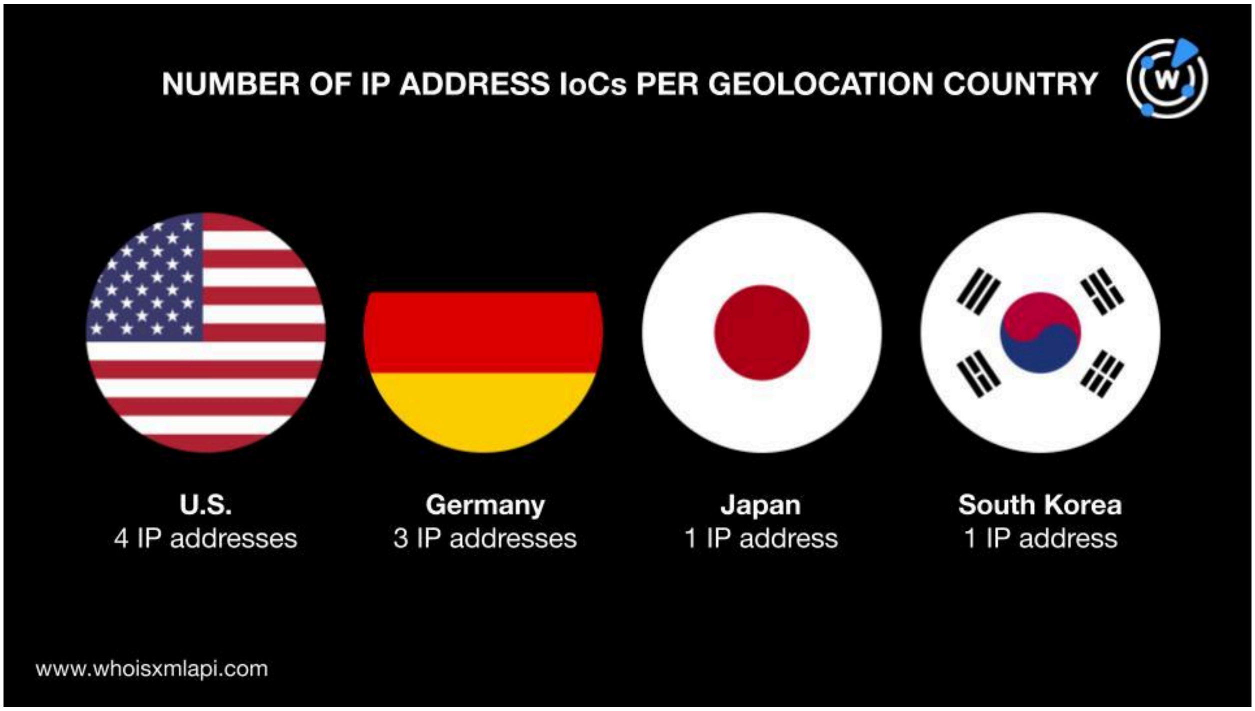


- One of them did not have registrant country data in its current WHOIS record while 122 were registered in the U.S.

The news-related text strings that appeared most among the 123 domain IoCs were **daily** and **post**. Each string appeared in nine domain names.

We then performed a bulk IP geolocation lookup for the nine IP addresses classified as IoCs and found that:

- They were geolocated in four countries—four in the U.S., three in Germany, and one each in Japan and South Korea.



NUMBER OF IP ADDRESS IoCs PER GEOLOCATION COUNTRY

U.S.
4 IP addresses

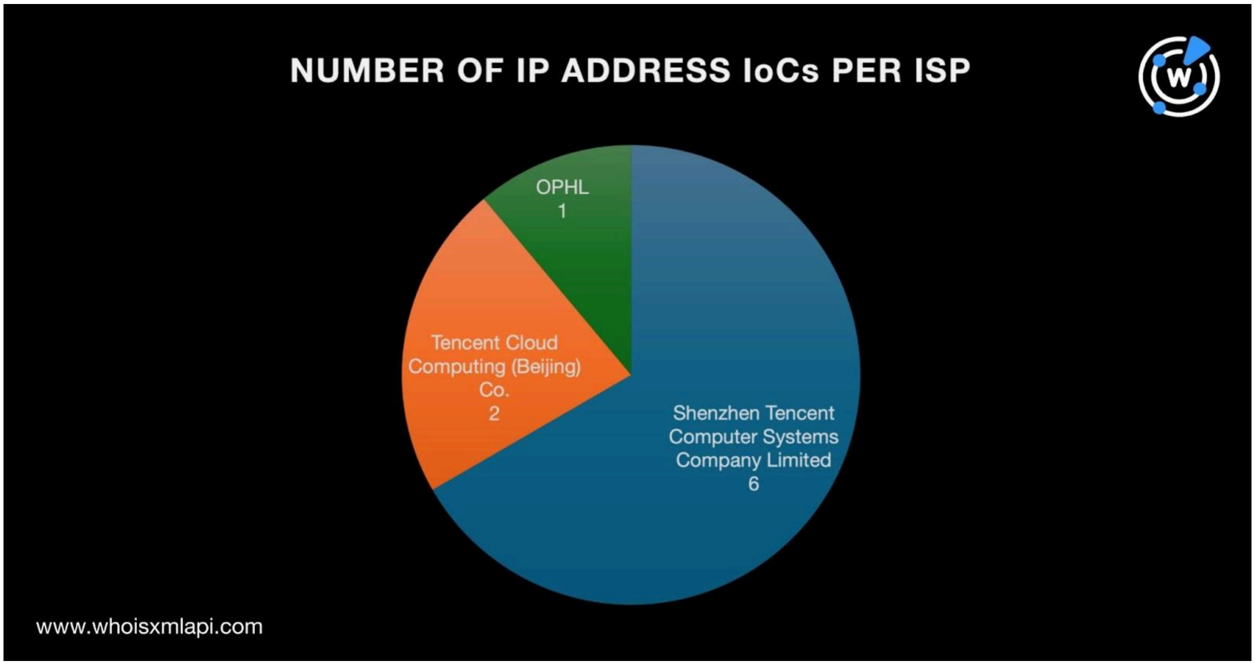
Germany
3 IP addresses

Japan
1 IP address

South Korea
1 IP address

www.whoisxmlapi.com

- They were distributed among three ISPs led by Shenzhen Tencent Computer Systems Company Limited, which accounted for six IP addresses. Tencent Cloud Computing (Beijing) Co. came in second place, administering two IP addresses, while OPHL handled one.



NUMBER OF IP ADDRESS IoCs PER ISP

www.whoisxmlapi.com

Search for PAPERWALL IoC-Connected Artifacts

To start off our in-depth analysis, we subjected the 123 domain names categorized as IoCs to WHOIS History API searches. They led to the discovery of 56 email addresses in their historical WHOIS records after duplicates were removed. Thirty-three were public email addresses.

We used the 33 unredacted email addresses as Reverse WHOIS API inputs. That allowed us to uncover 681 email-connected domains based on their current WHOIS records after removing duplicates and the IoCs.

It is also interesting to note that 103 of the email-connected domains contained news-related text strings akin to the domains tagged as IoCs. Sixty-four of them, in fact, had the string **diario**, a Spanish word for "diary" or "daily" and a term commonly used to refer to a newspaper. The other news-related text strings found among the connected domains include:

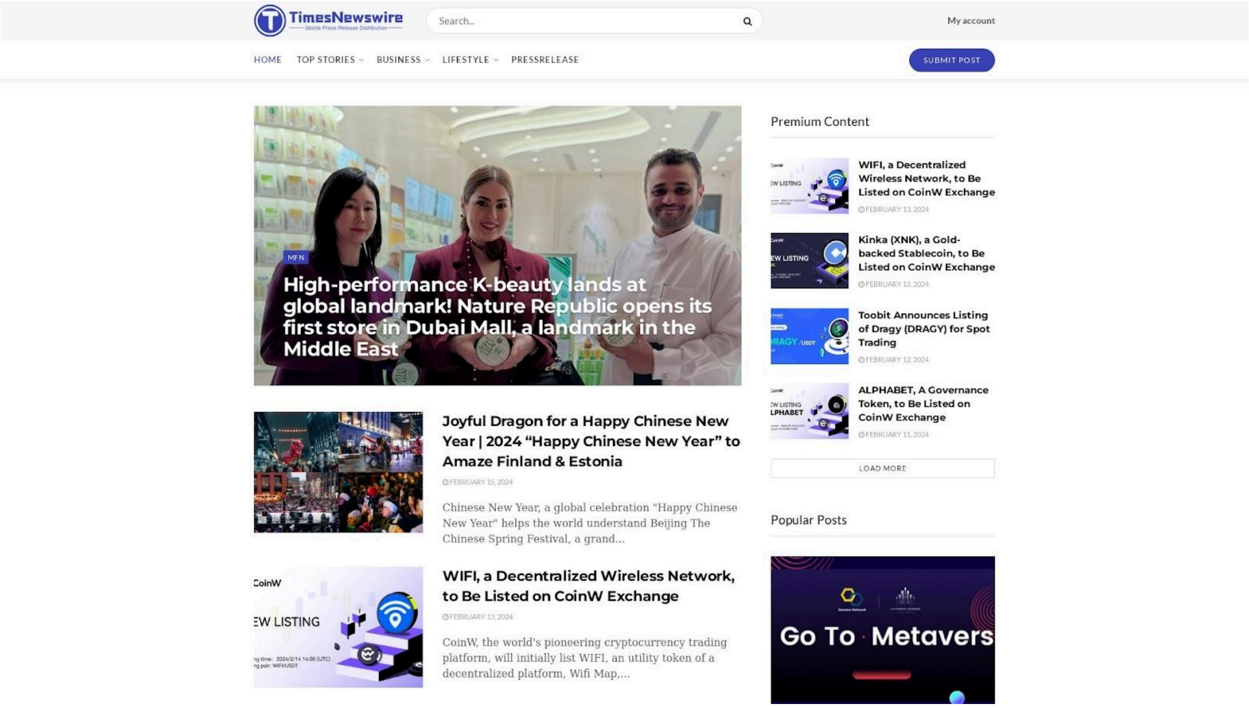
- **critic**
- **daily**
- **desk**
- **dia** (Spanish word for "day")
- **global**
- **government**
- **journal**
- **magasin** (Filipino word for "magazine")
- **magazine**
- **monthly**
- **paper**
- **periodico** (Spanish word for "newspaper")
- **press**
- **radio**
- **television**
- **today**
- **video**
- **weekend**
- **writer**

None of the email-connected domains contained the string **post,** which was present among the IoCs, though.

Screenshot API also revealed that seven of the email-connected domains continued to point to live pages although none seemed to lead to a news feed.

Next, we used the 123 domains named as IoCs as DNS Lookup inputs and found one additional IP address—128[.]14[.]74[.]124. Like a majority of the IP addresses identified as IoCs, it was geolocated in the U.S. It was, however, administered by an ISP that is not on our previous list, that is, Zenlayer, Inc.

Reverse IP lookups for the 10 potentially dedicated IP addresses we collated (i.e., nine IoCs and one additional host) uncovered one IP-connected domain—timesnewswire[.]com—after duplicates, the IoCs, and email-connected domains were filtered out. This connected domain was the one HaiEnergy used in attacks according to The Citizen Lab and Mandiant. It remains accessible to date and continues to host news updates.



High-performance K-beauty lands at global landmark! Nature Republic opens its first store in Dubai Mall, a landmark in the Middle East

Joyful Dragon for a Happy Chinese New Year | 2024 “Happy Chinese New Year” to Amaze Finland & Estonia

FEBRUARY 15, 2024

Chinese New Year, a global celebration "Happy Chinese New Year" helps the world understand Beijing The Chinese Spring Festival, a grand...

WIFI, a Decentralized Wireless Network, to Be Listed on CoinW Exchange

FEBRUARY 13, 2024

CoinW, the world's pioneering cryptocurrency trading platform, will initially list WIFI, an utility token of a decentralized platform, Wifi Map,...

Premium Content

WIFI, a Decentralized Wireless Network, to Be Listed on CoinW Exchange

FEBRUARY 13, 2024

Kinka (XNK), a Gold-backed Stablecoin, to Be Listed on CoinW Exchange

FEBRUARY 12, 2024

Toobit Announces Listing of Dragy (DRAGY) for Spot Trading

FEBRUARY 12, 2024

ALPHABET, A Governance Token, to Be Listed on CoinW Exchange

FEBRUARY 11, 2024

Popular Posts

Screenshot of the page hosted on IP-connected domain timesnewswire[.]com

As our final step, we trooped to Domains & Subdomains Discovery to look for domain names containing text strings found among the domain IoCs, namely:

- **alpsbiz.**
- **bohemiadaily.**
- **cctimes.**
- **cordovapress.**
- **dkindustry.**
- **doloreshoy.**
- **euleader.**
- **friendlyparis.**
- **fukuoka-ken.**
- **gwangjuedu.**
- **kanagawa-ken.**
- **kazanculture.**
- **londonclup.**
- **louispress.**
- **nlpress.**
- **romajournal.**
- **rostovlife.**
- **saitama-ken.**
- **samaraindustry.**
- **sanrafaelscoop.**
- **seoulpr.**
- **stptb.**
- **updatenews.**
- **usa-aa.**
- **vikingun.**
- **volgogradpost.**
- **vtnay.**
- **wakhan.**

- **wdpp.**

We found 193 string-connected domains after duplicates, the IoCs, and email- and IP-connected domains were removed. One of them—updatenews[.]me—turned out to be associated with a malware attack, according to Threat Intelligence API results.

Screenshot API also showed that 57 of them remain accessible as of this writing. Seventeen of the string-connected domain names led to what looked like news feeds, which could be abused for spreading propaganda.

Signs of Other News-Related Domains

Earlier, we mentioned three generic news-related text strings that appeared most among the IoCs and connected domains—**daily**, **post**, and **diario**. But since **post** could also figure in domains related to postal services, we only focused on **daily** and **diario**, which are more likely to point to sites bearing similarities to those identified as PAPERWALL IoCs.

Domains & Subdomains Discovery unveiled 5,277 domain names containing the string **daily** created since 1 January 2024. Threat Intelligence API queries showed that five of them were malicious. Four, in particular, were associated with phishing while one with a malware attack.

Our search for other **diario**-containing domains created since 1 January 2024, meanwhile, found 289 such web properties.

—

Our closer look at the 132 IoCs related to the ongoing propaganda campaign led to the discovery of 876 potentially related web properties—681 email-connected domains, one additional IP address, one IP-connected domain, and 193 string-connected domains. While only one of them, string-connected domain updatenews[.]me, is already considered malicious to date, the other possibly related web properties could also be abused to spread misinformation.

We also noted the presence of thousands of domains that could play host to similar malicious activities using only two of many possible text strings in the DNS.

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

- 0500london[.]org
- 0800london[.]org
- 121w[.]org
- 17tvmall[.]org
- 17tvos[.]org
- 24hourlondon[.]org
- 865623333[.]org
- aberdeenairporthotels[.]org
- acabadosaeroprint[.]com
- accaoimediata[.]pt
- accommodationlondon[.]org
- aceitetorredonjimeno[.]com
- adegcostadelsol[.]com
- aircmosventas[.]com
- alimentacioneuropea[.]com
- americaaffiliate[.]org
- americadata[.]org
- americaexperts[.]org
- americaknowledge[.]org
- americamaps[.]org
- andalucia[.]catering
- andalucia[.]consulting
- andalucia[.]sexy
- andaluciagay[.]org
- approbuilder[.]com
- apvherreriaalex[.]com
- artebird[.]info
- artedemarruecos[.]com
- artetheadbird[.]info
- artslondon[.]org
- attractionslondon[.]org
- auctionscostadelsol[.]com
- autocaresluna[.]mobi
- axbz[.]org
- bailegay[.]com
- barneshotels[.]org
- bddos[.]org
- bedfordshirehotels[.]org
- benidormhomosexual[.]com
- berkshirehotels[.]org
- besthighchair[.]org
- bexleyhotels[.]org
- biarritzgay[.]com
- bitxigarbiketak[.]com
- bjzyz[.]org
- blackheathhotels[.]org
- bogotagay[.]org
- bomberosmagazine[.]com
- brentfordhotels[.]org
- britaindata[.]org
- britainmarketing[.]org
- britainuniversities[.]org
- budgetlondon[.]org
- campeonatodelmundodecine[.]com
- campeonatodelmundodefilms[.]com
- carnicascarrion[.]com
- carpinteriabasalum[.]com
- carpinteriafranciscosoriano[.]com
- carpiteriametalicaperez[.]mobi
- carrentallondon[.]org

- carskiss[.]com
- casamasip[.]mobi
- casaruralogonomendi[.]com
- centraldecomprasgays[.]com
- centroeuropeodecongresos[.]com
- certamendebomberos[.]com
- chinaseafood[.]org
- chingfordhotels[.]org
- chislehursthotels[.]org
- chiswickhotels[.]org
- chlgrupo[.]net
- cinegaycostadelsol[.]com
- circulofinancierointernacional[.]com
- claphamhotels[.]org
- clevelandsurvey[.]org
- clinicadentalgabrielrubio[.]com
- cnrmb[.]org
- coachcompanies[.]org
- coches56[.]com
- cofradiasenred[.]com
- colegatorremolinos[.]com
- comemelapolla[.]org
- comerhoy[.]net
- contenedoresurbil[.]com
- conventionlondon[.]org
- cordesalinas[.]com
- cortijoaltozano[.]com
- cpdesk[.]ca
- cpdesk[.]us
- croftonpark[.]org
- crouchend[.]org
- crystalpalacehotels[.]org
- cubiertasmiguelmartinez[.]com
- cubiertasytejadosdepizarraenasturias[.]com
- cundian[.]org
- customrubixcube[.]org
- dailylondon[.]org
- derbyshirehotels[.]org
- desguaceluqueislamayor[.]com
- desinsectacionesenmarbella[.]com

Sample String-Connected Domains

- alpsbiz[.]site
- bohemiadaily[.]cz
- bohemiadaily[.]eu
- cctimes[.]ca
- cctimes[.]cc
- cctimes[.]club
- cctimes[.]cn
- cctimes[.]co[.]kr
- cctimes[.]co[.]uk
- cctimes[.]com
- cctimes[.]com[.]au
- cctimes[.]com[.]cn
- cctimes[.]date
- cctimes[.]gift
- cctimes[.]help
- cctimes[.]info
- cctimes[.]kr
- cctimes[.]link
- cctimes[.]mobi
- cctimes[.]net
- cctimes[.]net[.]cn
- cctimes[.]news
- cctimes[.]online
- cctimes[.]pub
- cctimes[.]ren
- cctimes[.]site
- cctimes[.]tech
- cctimes[.]top
- cctimes[.]vip
- cctimes[.]win
- cordovapress[.]com
- dkindustry[.]co[.]kr

- dkindustry[.]co[.]za
- dkindustry[.]com
- dkindustry[.]in
- dkindustry[.]net
- dkindustry[.]org
- doloreshoy[.]com
- euleader[.]com
- euleader[.]com[.]br
- friendlyparis[.]fr
- friendlyparis[.]org
- friendlyparis[.]xn--fiqs8s
- friendlyparis[.]xn--fiqz9s
- fukuoka-ken[.]jp
- gwangjuedu[.]co[.]kr
- kanagawa-ken[.]jp
- kanagawa-ken[.]net
- kazanculture[.]ru
- londonclup[.]xyz