WhoisXMLAPI
The Who Behind Domain, IP & Cyber Threat Intelligence

WHITE PAPER

DNS Abuse Trends: Dissecting the Domains Under the Most Abused TLDs

Contents

Executive Summary

The Internet Corporation for Assigned Names and Numbers (ICANN) defines DNS abuse as "any malicious activity that disrupts or misuses the DNS infrastructure, including related protocols, services, and domain names."

DNS abuse can be broadly categorized into malware, botnet, phishing, pharming, and spamming attacks. These are the most rampant threat activities—some of which, such as spamming, phishing, and malware attacks, have become household names.

With countless DNS properties and services that threat actors can weaponize, combating DNS abuse is quite challenging. Keeping track of threats requires collective effort among members of the cybersecurity community.

WhoisXML API built on Spamhaus's list of the 10 most-abused top-level domains (TLDs) in this report to shed light on domains linked to TLDs with the worst reputation for spamming. Our researchers analyzed more than 391,000 domains added in the fourth quarter of 2022 that sported TLDs that appeared on the Spamhaus list from November 2022 to January 2023. Our analysis revealed the following:

- About two-thirds of the domains had redacted WHOIS records, making threat attribution challenging if they figure in malicious campaigns.
- The top registrars administering the domains were Alibaba Cloud Computing Limited and NameSilo, accounting for 30% of the total registration volume.
- The leading ISP of the resolving domains was Cloudflare, with a 21% share of the total IP resolution volume.
- The domain registrations and IP resolutions could mostly be traced to the U.S. and China.
- Several domains contained gambling-related text strings and popular company names.

2

Methodology and Tools

WhoisXML API produces a monthly newsletter that looks into domain registration activities and trends for a particular month. This study is a more targeted edition of the monthly newsletter. Instead of probing newly registered domains (NRDs) across all TLDs, the researchers focused on 10 of the most-abused TLDs, namely:

- .surf
- .live
- .cn
- .beauty
- .fit
- .top
- .degree
- .su
- .link
- .garden

The list of the most-abused TLDs constantly changes. Even with such ranking, other TLDs are not foolproof since threat actors can weaponize any domain under any TLD. That said, the data collection and analysis were performed using the following intelligence tools:

- Reverse WHOIS Search to obtain a list of domains under each TLD added each week from 1 October to 31 December 2022
- Bulk WHOIS Lookup to retrieve the complete WHOIS information of a randomized sample
- Bulk IP Geolocation to determine the ISP and geolocation distribution of a randomized sample
- Domain Malware Check API to identify which domains from the sample have already been reported as malicious
- Screenshot API to see the type of content hosted on the domains

3

Data Analysis and Findings

Out of 391,631 domains sporting the 10 most-abused TLDs added in Q4 2022, the researchers took a random sample of 40,000 domains. They then processed the properties to determine their WHOIS redaction status, administering entities, registrant countries, IP geolocation, and most-used text strings. The findings are detailed below.

A. State of WHOIS Redaction of the Most-Abused TLDs

WhoisXML API researchers have been detecting growth in WHOIS data redaction since its implementation. In December 2022, around 70% of the NRDs had redacted WHOIS records, akin to the domains under the most-abused TLDs. About 64% had redacted or privacy-protected WHOIS records based on their registrant names.

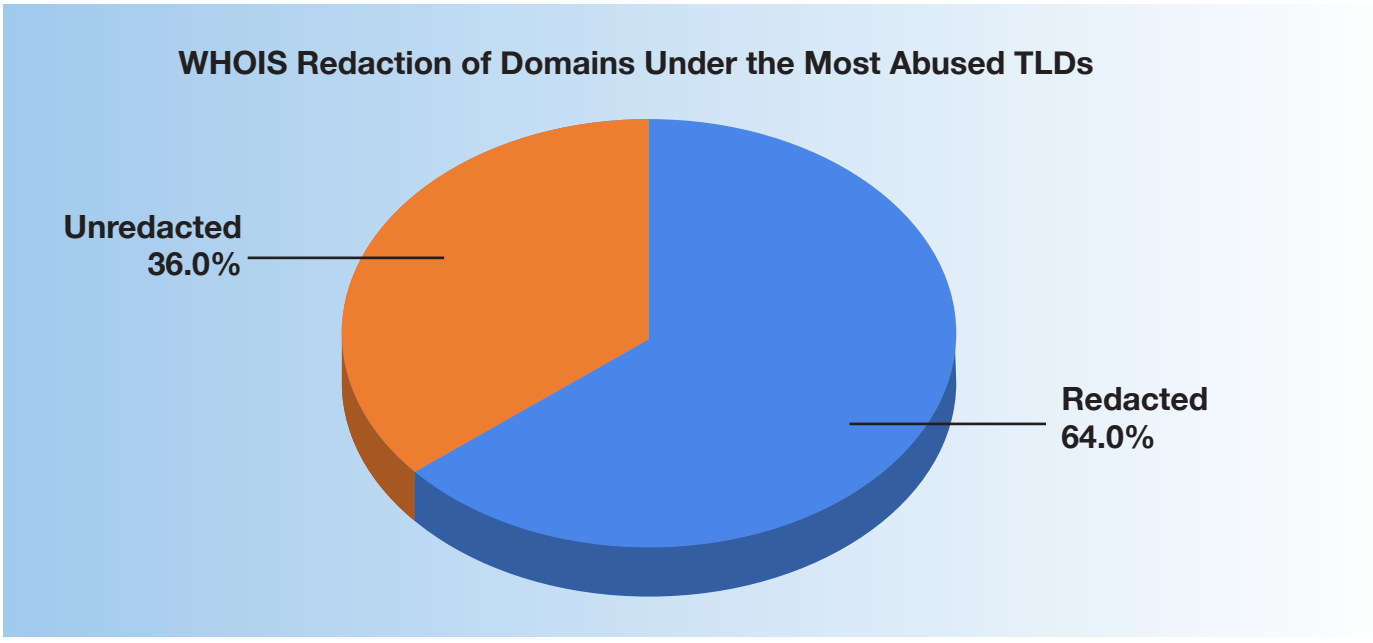


Figure 1: *Ratio of domains with redacted WHOIS records against those with public WHOIS data*

The remaining domains had public registrant names, but less than 1% of the sample had public registrant email addresses. While widespread WHOIS data redaction can be problematic to the cybersecurity community, the DNS can still provide traces that can lead to malicious infrastructures and actors. The subsequent analyses are examples of such paths to uncovering clues.

B. What Entities Administered the Domains?

Among the first questions to address is the "who" behind the properties under the TLDs with the worst reputations. Given that their registrant contact details were mostly redacted for privacy, we turned to their registrars and ISPs, as these entities could help take action against the malicious properties on their turf.

Registrar Distribution

Alibaba Cloud Computing Limited was the top registrar, accounting for 18% of the total domain registration volume. NameSilo followed with 12%, Chengdu Xiwei Digital Technology Co., Ltd. with 9%, Namecheap with 8%, GoDaddy with 7%, Chengdu West Dimension Digital with 5%, and Name.com, Inc. with 3%. 1API GmbH, Jiangsu Bangning Science & Technology Co. Ltd., and Zhengzhou Century Chuanglian Electronic Technology Development Co. Ltd. each accounted for 2% of the domain registrations.

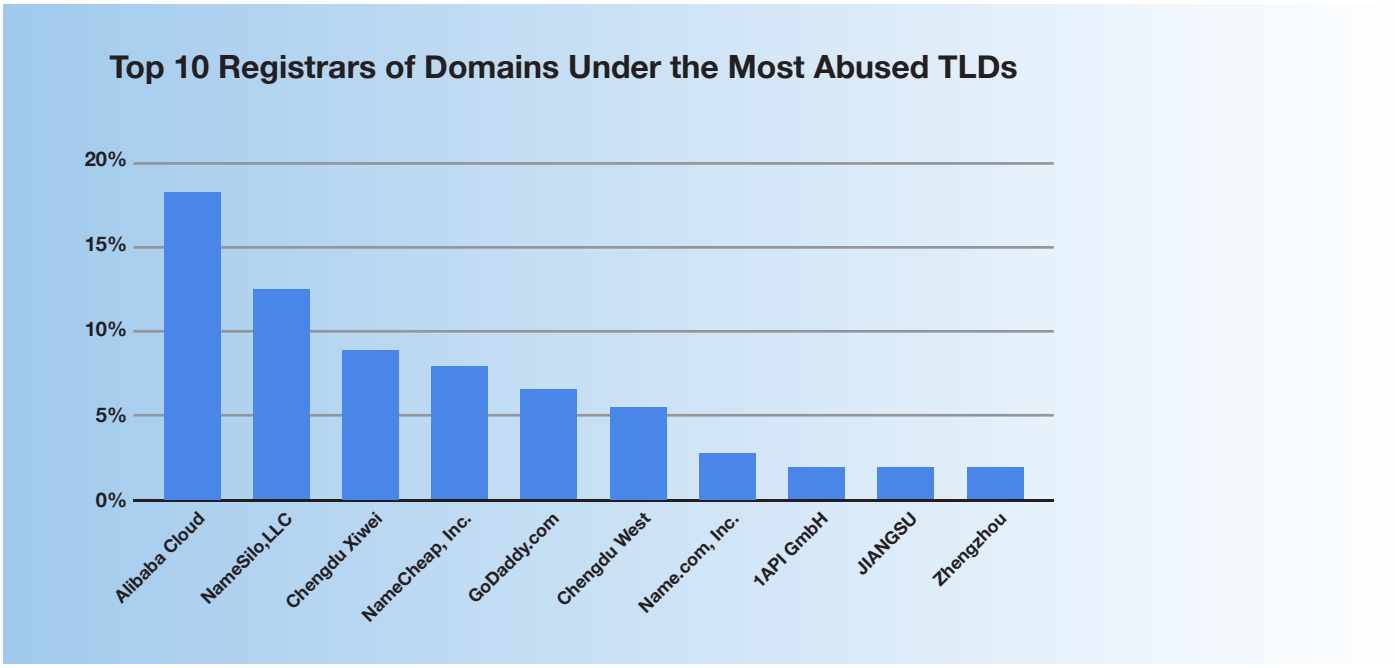


Figure 2: *Top 10 registrars of domains under the most-abused TLDs*

The top 10 registrars accounted for 68% of the total domain registration volume. The remaining 32% were distributed across 257 other registrars from around the globe.

ISP Distribution

Only about 63% of the sample had active IP resolutions. The researchers determined that 21% of these resolutions could be traced to Cloudflare. The other top ISPs only accounted for 4% or less of the resolutions each. Amazon and Google each had a 4% resolution share, followed by Servers.com with 3%; SEDO, FranTech Solutions, Peg Tech Inc., and DignFeng XinHui with 2% each; and Namecheap and Cnservers LLC with 1% each. The rest of the resolutions were distributed across 987 other ISPs.

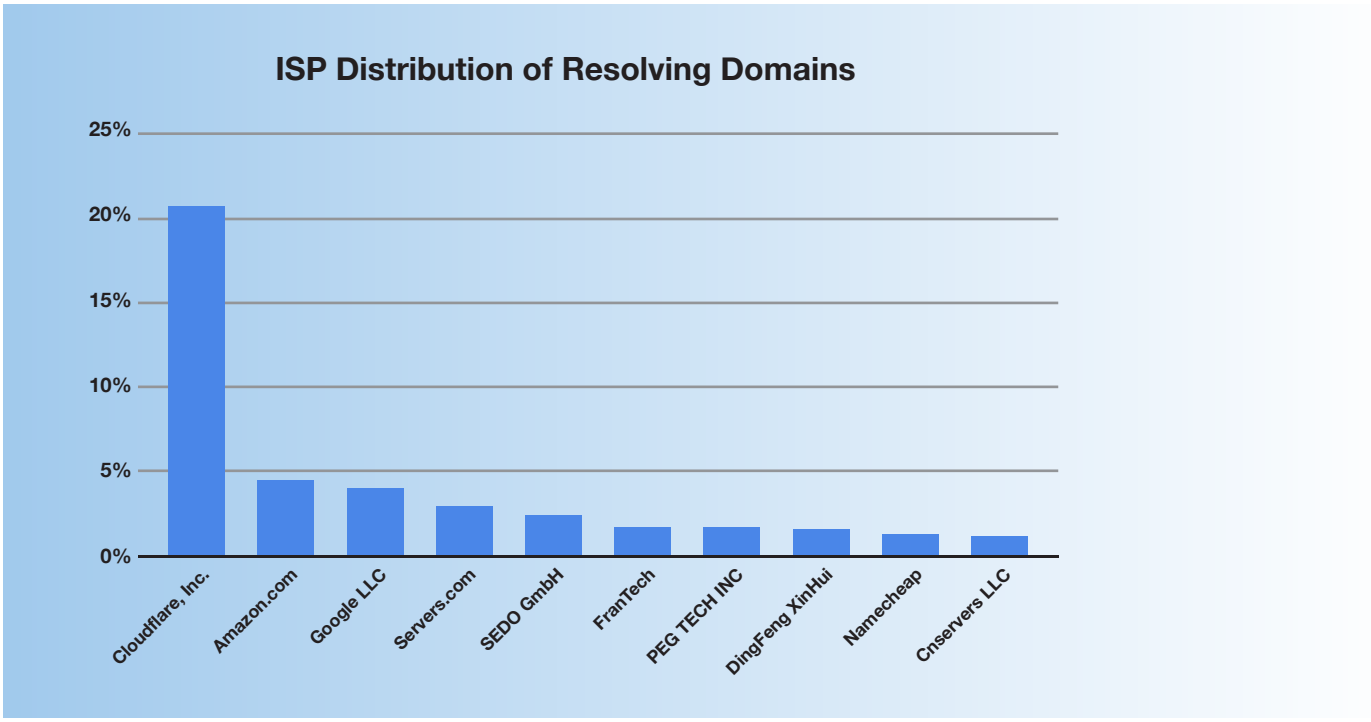


Figure 3: *Top 10 ISPs of resolving domains under the most-abused TLDs*

C. Where Are the Domains Located?

WHOIS and DNS intelligence gave the researchers a glimpse of the domains' top locations in terms of registration and resolution. These are detailed below.

Registrant Country

The U.S. accounted for most of the domain registrations with 28%, followed by China with 20%. The rest of the top 10 registrant countries are mapped out in the image below.

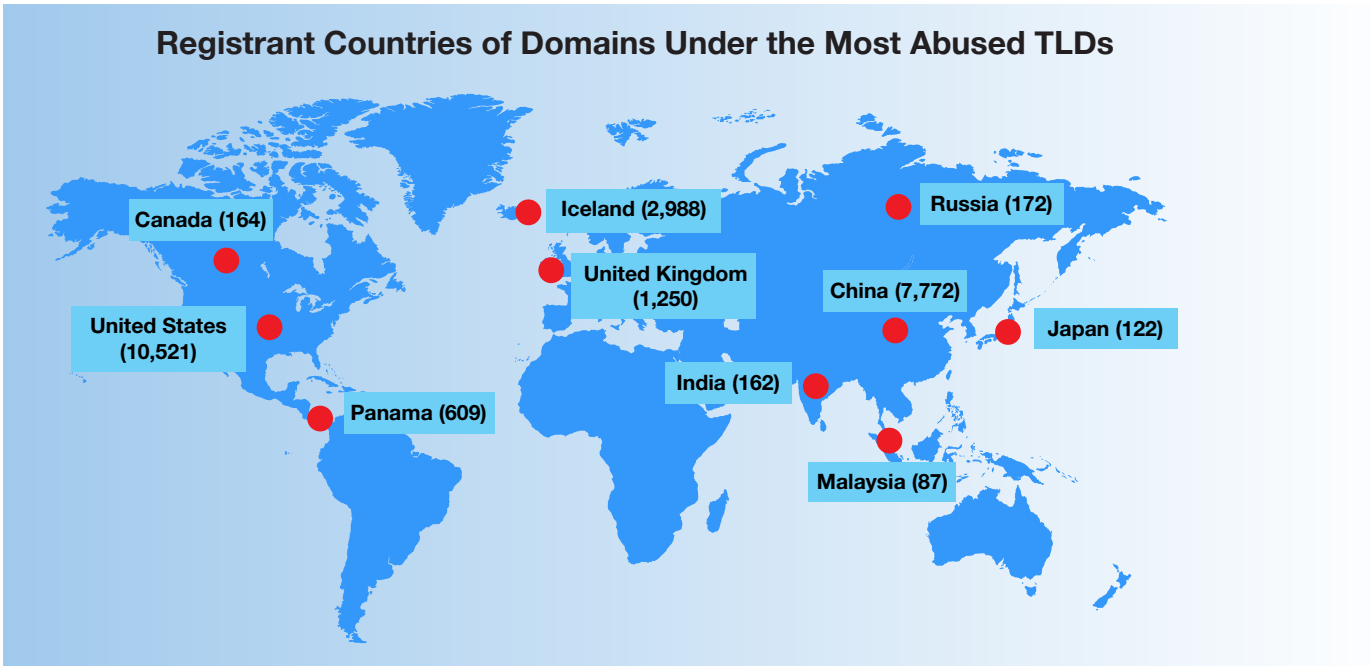


Figure 3: *Map showing the top 10 registrant countries of the domains under the most-abused TLDs*

IP Geolocation

Similarly, the U.S. accounted for a massive 67% of the reported IP resolutions. China came in second with 15%, while the rest were distributed across 60+ countries worldwide. The top 10 IP geolocation countries can be seen in the map below, along with their respective number of IP resolutions.

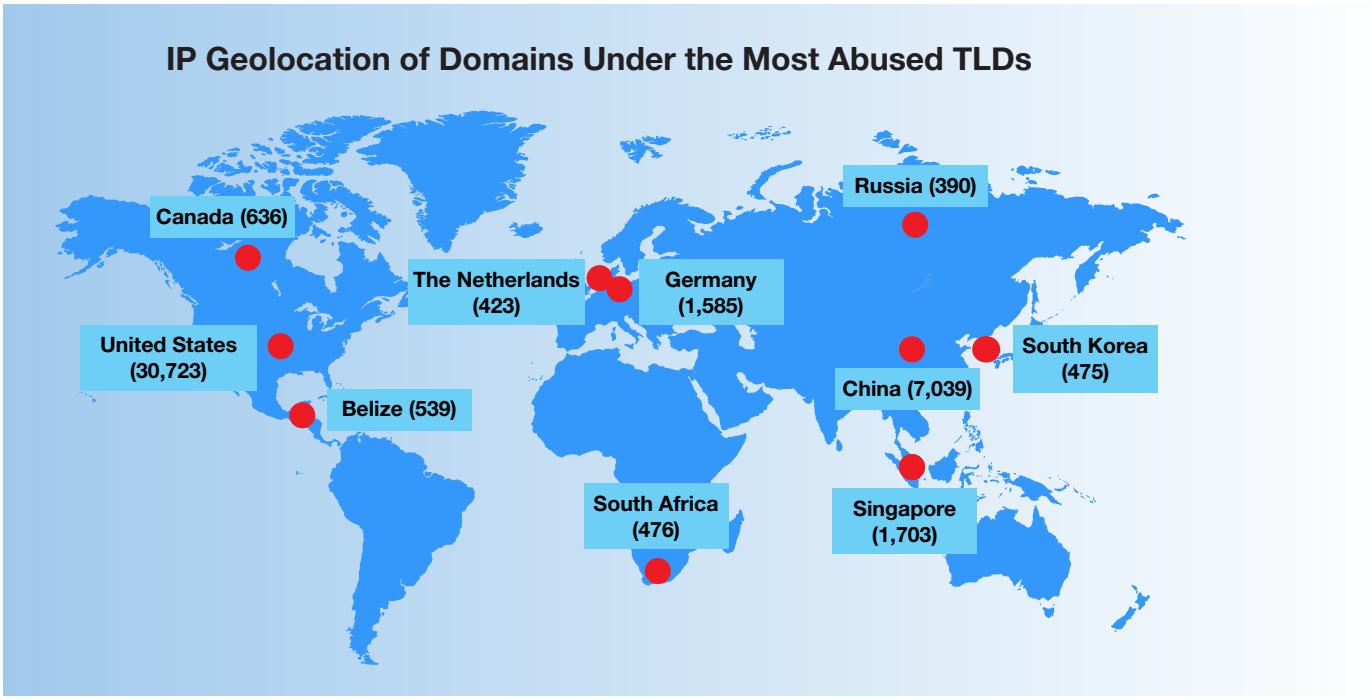


Figure 5: *Top 10 IP geolocation countries of the resolving domains under the most-abused TLDs*

D. What Text Strings Were Commonly Used in the Domains?

The researchers detected the rampant use of two-letter strings—***ok, an, be, in,*** and ***do*** —alongside dashes (-) and other strings, based on a lexical analysis of a random sample of 1,000 domains. In fact, about 7% of the sample contained dashes, with several trying to cram a phrase into the domains in an effort to make sense. Some examples include:

- add-an-intl-scholarships-ok[.]live
- do-an-intl-car-rentals-big[.]live
- holidays-tourist-apartment-zurich[.]top
- ok-in-serviced-apartment-hong-kongs-ok[.]live

Other domains sported typo variants of popular company and brand names, using dashes to appear legitimate. Here are a few examples:

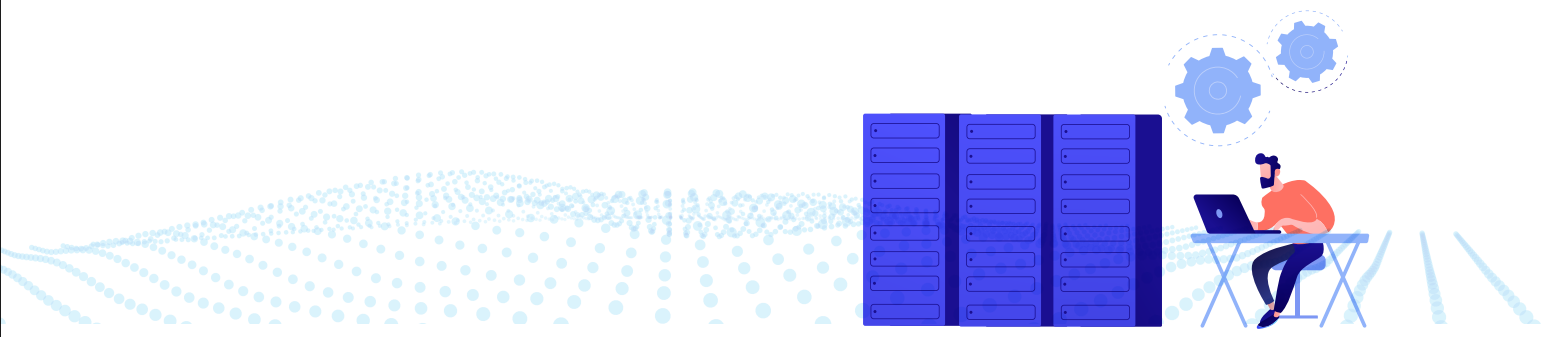
- i-apple-care[.]live
- mylost-apple-maps[.]live
- newattempt-usps[.]top
- sharepoint-microsoftonline[.]live
- upsed9865-usps[.]link
- usps--usps[.]top

Location keywords, such as ***US, Cyprus,*** and ***Dubai*** also appeared in most of the domains. These and other recurring strings are shown in the word cloud below.

Figure 6: *Word cloud showing the widely recurring text strings among the domains*

The repeated appearance of ***xn*** indicates that internationalized domain name (IDN) usage was quite popular among the most-abused TLDs in Q4 2022. That has been the case for a few months now, and the trend will likely continue.

Hundreds of domains also contained numeric characters. Lastly, the words ***bet, casino,*** and other gambling-related strings appeared in more than 500 domains. A list of the top 100 strings is available in the Appendix.

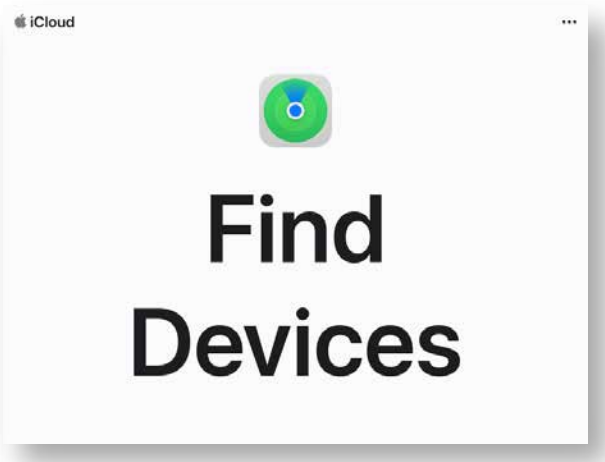


E. What Did These Domains Host?

Several domains were either parked or resolved to 404 pages. Some also hosted account suspension notices.

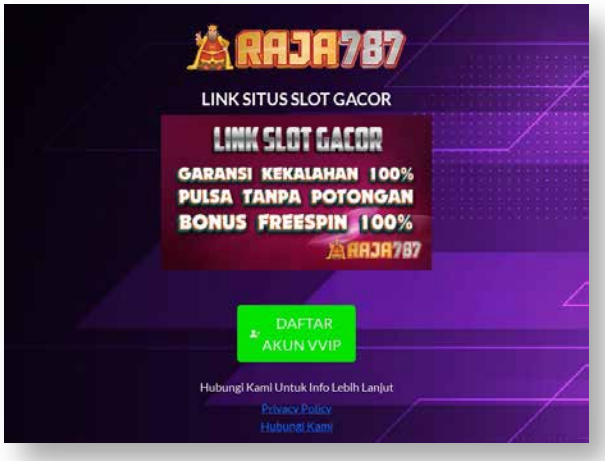
However, what stood out were domains that continued to host live websites with content despite being flagged as malicious. For example, window[.]su still appeared to offer cracked versions of software, while supp-p[.]live continues to host content imitating iCloud. These and other examples are shown below.

Screenshot of window[.]su



Screenshot of supp-p[.]live

Screenshot of sofrport2022[.]su



Screenshot of panjianlian[.]live

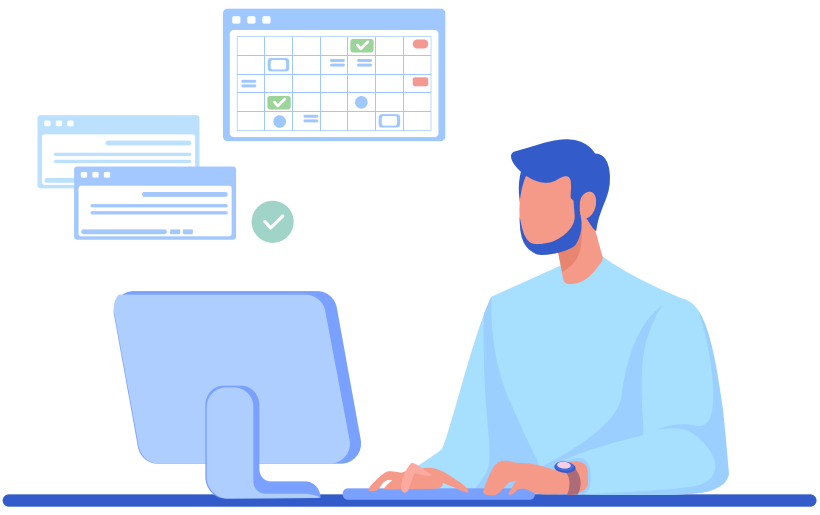
4

The DNS as a Rich Threat Intelligence Source

The DNS is prone to abuse. The increasing number of cases of phishing, spam, and malware distribution campaigns can attest to that. But the DNS is also a reliable source of threat information, which can be probed to process, analyze, and mitigate online dangers.

Despite massive data redaction, WHOIS and DNS data points can provide clues for expanding lists of IoCs, threat actor monitoring, and other detection and response processes. These intelligence sources can help the cybersecurity community look beyond privacy redaction and into name server resolutions, IP host connections, historical ownership records, geolocation details, and other digital footprints.

Are you interested in monitoring domain registration trends associated with TLDs affected by poor reputation? Feel free to **contact us** for more information about our products and capabilities.



Appendix

Top 100 Recurring Strings

String	Volume	String	Volume	String	Volume	String	Volume
Ok	170	Car	18	The	11	Sh	8
Xn	169	Support	18	Casinox	11	Ask	8
In	101	Moneyeasily	18	He	11	One	8
Intl	90	Usps	16	Post	11	Sz	8
An	66	Melbet	15	Download	11	And	8
Us	63	Pokerdom	15	Eldoradocasino	11	Hd	8
Cyprus	59	To	15	All	10	Jobs	8
Investing	55	Info	15	Store	10	Holidays	8
Be	46	Apple	15	Edu	10	Server	8
Usp	43	Rentals	14	Device	10	Fast	8
Do	42	Playfortuna	14	Data	10	Hug	8
Online	37	Shop	14	Girls	10	Add	8
Joycasino	36	Hb	14	Courses	10	Pro	8
1xbet	35	Marketing	14	1xslots	9	Hotel	7
Go	34	Catcasino	13	Azino777	9	Re	7
It	31	App	13	Design	9	Cn	7
Com	29	Help	13	Tech	9	Ads	7
Dubai	28	India	13	Hub	9	Bay	7
Usa	28	Cloud	13	Now	9	Quickbooks	7
Coto	26	Web	13	My	9	Study	7
Villas	24	Vavada	12	Of	9	On	7
Mostbet	22	Casino	12	Scholarships	9	Smart	7
Wallboard	22	Digital	12	Ray	9	Onl	7
Intls	21	New	11	Top	9	Admiralx	7
Ms	20	Find	11	Home	9	Sg	7

Sample Malicious Domains Flagged as of 31 January 2023

- cardsexmed[.]live
- liks[.]live
- center-credisis[.]top
- digitale-no[.]top
- walkjoben[.]live
- linethencash[.]live
- mshub23[.]live
- oydrewgrow[.]live
- us-psdoa[.]top
- ps1ujajz[.]top
- chosenstar[.]cn
- us-zvaqw[.]top
- u-psizaje3e[.]top
- canscelledupdate[.]top
- mistocd[.]top
- icesendate[.]live
- urehssa[.]top
- countryanonymity[.]top
- particularesdigital[.]live
- hoskinpeak[.]live
- igdd[.]top
- upps[.]live
- us-psdocd[.]top
- debtareatime[.]live
- louter[.]live
- finds-mydevices[.]live
- gymampcab[.]live
- numerousdrum[.]top
- idstore[.]live
- ubuntuhubs[.]top
- hvbaxaz[.]top
- emailadmin[.]com[.]cn
- ledus[.]live
- aspirational[.]live
- netagentinfo[.]top
- 1academia-vendas[.]top
- aidsscrub[.]cn
- mughawk[.]cn
- senatordefault[.]cn
- mybell[.]live
- digitalonliinejdcu[.]top
- anlav[.]live
- jerton[.]live
- awe-ggl-adv-inds-ok[.]live
- chitgenerousmatter[.]beauty
- zxdjtswb[.]top
- uspo2[.]top
- zhyat[.]top
- x-pay[.]top
- biashomo[.]cn
- presenceuranium[.]cn
- onlinereview[.]live
- caterlimp[.]cn
- panjianlian[.]live
- fores[.]live
- celis[.]live
- xdszaq[.]top
- ological[.]beauty
- nistrrsion[.]beauty
- tang2002wei0308[.]top
- rhyw12[.]top
- mail-saverscloudbackedup[.]top
- sjbpt[.]top
- likeru[.]live
- mobileworkscg[.]top
- ecosystempamphlet[.]top
- bzuxfd[.]beauty
- correlationjelly[.]cn
- daysremote[.]top
- immenselysuffice[.]top
- waondly[.]live
- faclosingdoc[.]top
- elrond[.]top
- gordonalanreynoldsjr[.]top
- mistored[.]top
- zulnar[.]cn
- webcriptarquivoseguros[.]beauty
- imdown[.]live
- aikido[.]fit
- micropartnerlink[.]top
- kzxl[.]link
- bookcom02023287487328748[.]top
- xxoozhuanvip695[.]top
- zsxcfv[.]top
- usp-spzws[.]top
- earopti[.]beauty
- wallapop-es[.]top
- dbsofficiat[.]top
- mistop[.]top
- weizaodai[.]cn
- wells-1protection[.]top
- verify-user2394869273926234[.]top
- tamirimumkun[.]live
- blitheblinn[.]top
- ifalhlzu[.]top
- diawu[.]cn
- fikojp[.]top
- mymt[.]live
- nived[.]live
- fishyu[.]top

About Us

WhoisXML API is a cyber intelligence provider that gives enterprises access to one of the largest repositories of well-parsed domain, subdomain, IP, and DNS data that enhances cybersecurity platforms' capabilities and helps security teams gain superior network security.

The data that WhoisXML API provides comes in different consumption models, ranging from APIs, data feeds, monitoring tools, and lookup tools, all of which make the Internet more secure and transparent. WhoisXML API has more than 50,000 satisfied customers, spanning law enforcement agencies, cyber forensics analysts, threat hunters, and cybersecurity solutions developers.