20 Questions WHOIS Data Can Help Answer

Posted on July 11, 2022

Aside from the most obvious and common WHOIS data use case—determining “who is” behind a domain—each WHOIS record can help reveal more details about a domain.

On a higher level, WHOIS information can provide hints about a domain name’s security, vulnerability, and lucrativeness, fueling critical security and business capabilities. When used alongside other data sources, it can enrich attack surface intelligence, security platforms, law enforcement solutions, and market intelligence.

On its own, WHOIS data can provide more context about a domain and help organizations make security and business decisions. From the creation and expiration dates to the registrar and technical contact details, every data point helps answer questions not only about a domain but also relevant to the organization behind it.

We listed more than a dozen of these questions below, categorizing them according to the type of data point, namely, domain age, domain infrastructure, and contact information.

Domain Age and Expiration Date

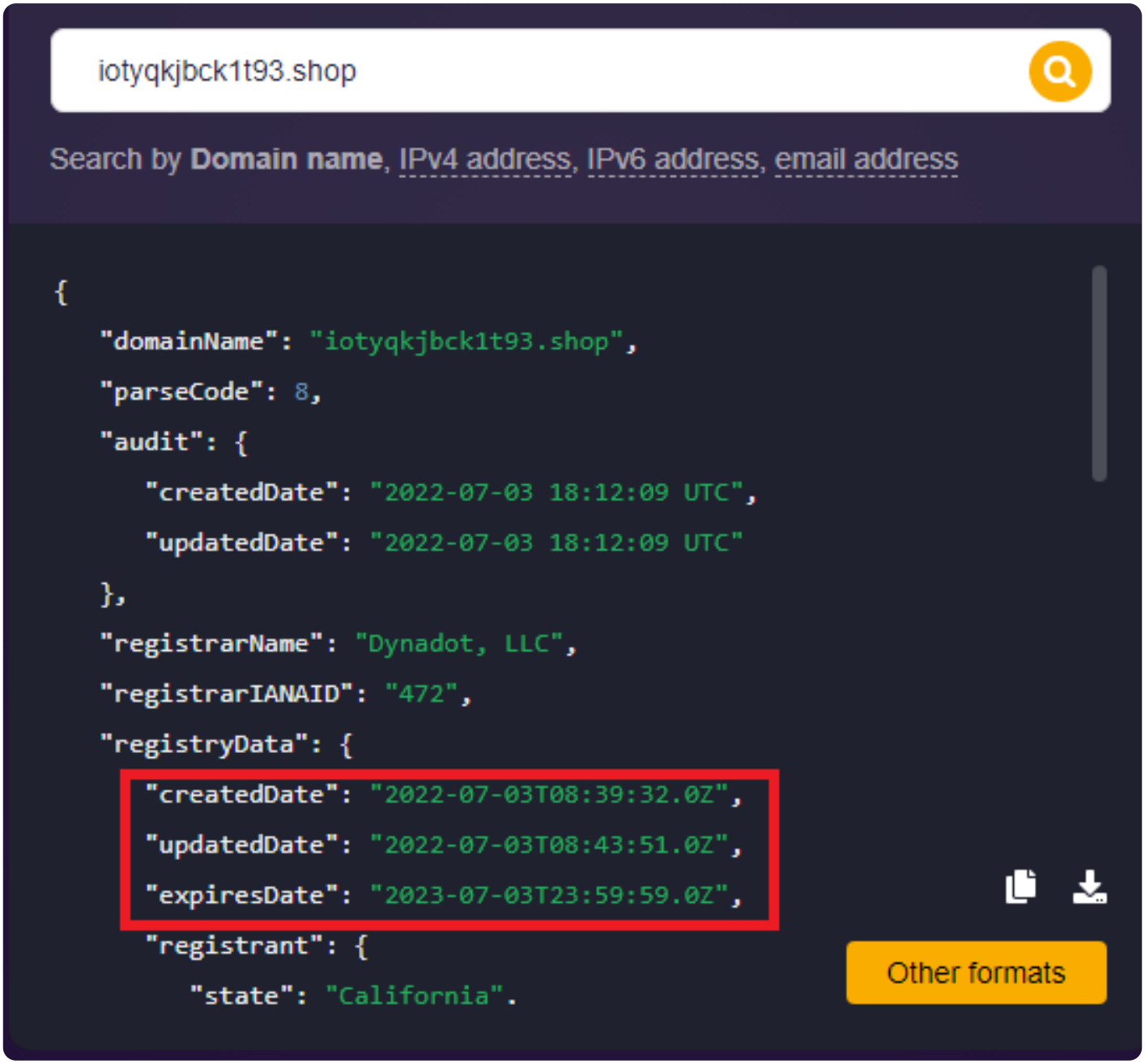
Domain age and expiration date are bundled in this category, as they both refer to a domain’s significant dates.

Domain Age

The domain age is determined by its creation date, although WHOIS API automatically calculates the age and displays it as part of WHOIS lookup results. This data point is significant when making

business and cybersecurity decisions.

For instance, organizations are generally wary of newly registered domains (NRDs) since threat actors have repeatedly weaponized them. At the time of writing, the domain iotyqkjbck1t93[.]shop is an example of a malicious NRD. It is a verified phishing domain reported on PhishTank a day after it was created on 3 June 2022. Below is a screenshot of its WHOIS record, including its creation and last update dates.



This and many other malicious NRDs prove that threat actors can use domains immediately after registering them. Therefore, knowing the domain age is crucial.

Expiration Date

On the other hand, a domain's expiration date tells administrators if it's time to facilitate its registration renewal. For other parties interested in the domain, the expiration date can signal the possibility of getting their hands on the target web property.

There are several ways the domain age and expiration date can help organizations. These are listed in the table below.

Notable Use Cases	Description
Establish the credibility of an organization	- How old is the company's domain? Does it match the details its representatives provided, such as length of business operation and license validation? - Does the domain age indicate the organization has enough experience in the field it specializes in?
Assess a domain's profitability	- How old is the domain and would this affect the organization's reach, given that most security tools block new domains? - Is the domain old enough to have an established domain authority and help promote the business on the Web?
Determine the domain's risk of undesired expiration	- When will the domain's registration expire? Is it time to renew its registration? - Has the domain expired? Can other parties swoop in and take over it?

The domain age and expiration date are simple yet very important data points. Advanced security solutions factor in a domain's age, which can often be an important clue that gives malicious domains away.

Expiration dates shouldn't be ignored either, as doing so can cause businesses to lose their

domains to competitors or brand impersonators.

Domain Infrastructure

WHOIS records contain data points that allow us to map the domain's infrastructure. Examples of such data points are registrar name, WHOIS server, nameserver, and status codes. They tell us the systems, networks, and organizations behind domain names.

Knowing these infrastructure details is crucial, as they can help assess the health of a domain and protect an organization from domain-associated digital risks.

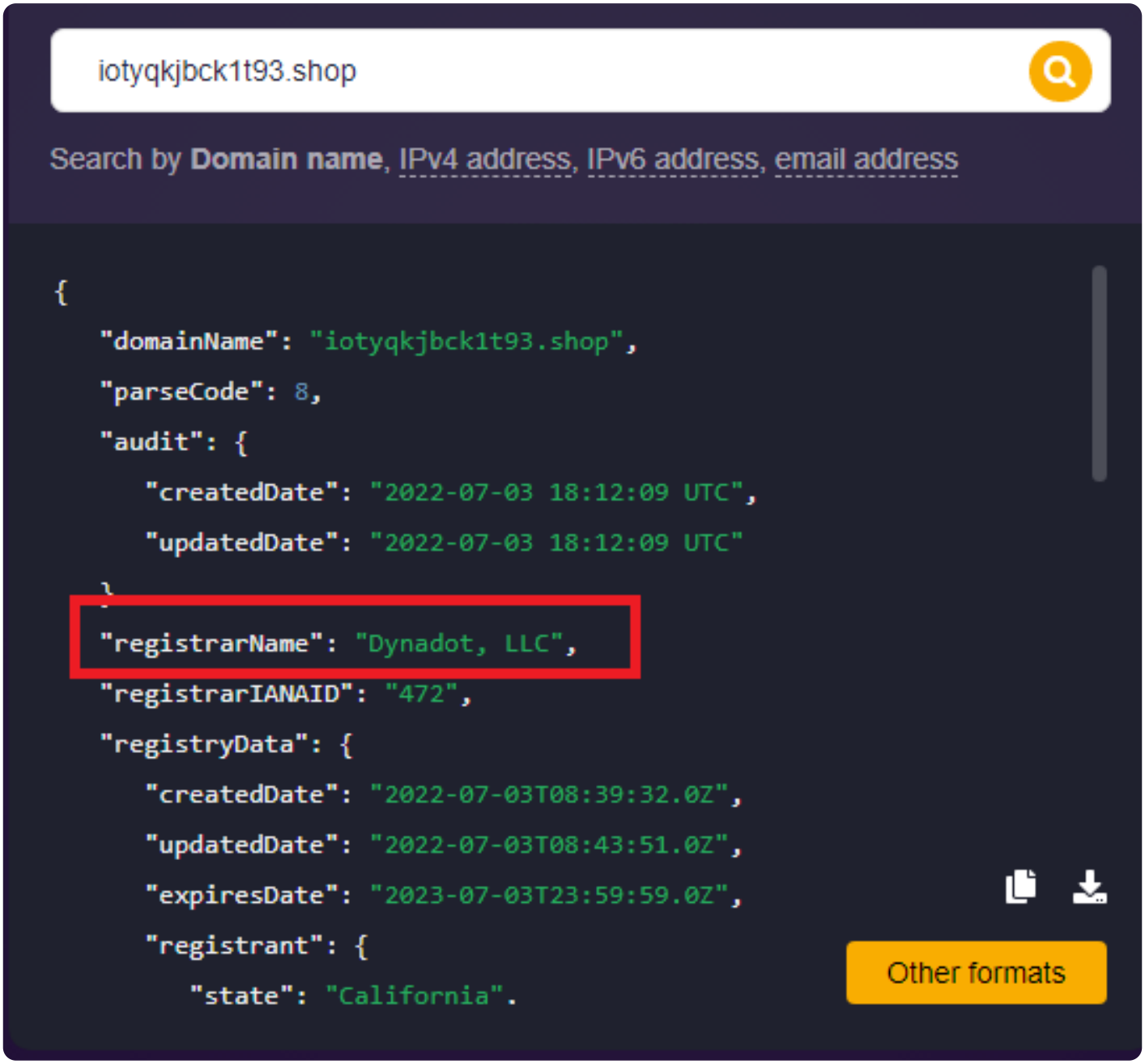
For one, some registrars and hosting providers may have less stringent anti-abuse requirements, making the domains they manage more vulnerable to attacks and exploitation. To illustrate, Spamhaus regularly publishes the top 10 most abused domain registrars.

The 10 Most Abused Domain Registrars

As of 04 July 2022 the registrars with the worst reputations for spam domains are:

1	**OwnRegistrar / Trunkoz**	Badness Index: **3.00** Domains seen: 7,629 Bad domains: 2,876 (**37.7%**)
2	**nicenic.net (ZhuHai NaiSiNiKe Information Technology)**	Badness Index: **2.87** Domains seen: 1,669 Bad domains: 728 (**43.6%**)
3	**Hongkong Domain Name Information Management**	Badness Index: **2.54** Domains seen: 1,047 Bad domains: 438 (**41.8%**)
4	**NameSilo**	Badness Index: **2.27** Domains seen: 70,468 Bad domains: 16,488 (**23.4%**)
5	**dnspod.cn (Guangzhou Yunxun Information Technology Co., Ltd. / 广州云讯信息科技有限公司)**	Badness Index: **2.19** Domains seen: 21,220 Bad domains: 5,408 (**25.5%**)
6	**Todaynic / Eranet International**	Badness Index: **2.07** Domains seen: 1,676 Bad domains: 550 (**32.8%**)
7	**Registrar R01.ru**	Badness Index: **2.00** Domains seen: 2,982 Bad domains: 878 (**29.4%**)
		Badness Index: **1.94**

While several legitimate and safe domains are managed by these registrars, more than 10% are considered bad domains. For Dynadot, the exact figure is 16.7%, meaning for every 20 domains, about 3–4 are malicious. Among them is the verified phishing domain we provided as an example above (iotyqkjbck1t93[.]shop), whose registrar is Dynadot.



In effect, domain infrastructure information enables organizations to answer security and vulnerability questions about domains, including those in the table below.

Notable Use Cases	Description
Determine the possibility of a domain going bad	- Who is the domain's registrar? Is the organization reputable or is it known for being susceptible to or less stringent about abuse? - What is the domain's nameserver? Has it figured in cyber attacks in the past? Are there indications that the nameserver is controlled by malicious actors?
Assess the vulnerability of the domain	- What hosting provider does the domain use? Has it been a target of cyber attacks in the past? Does the provider have security systems in place to protect clients against denial-of-service (DoS) and other cyber attacks? - What status codes are indicated? Do the domain's statuses provide an additional layer of protection against unauthorized transfer, deletion, and takeovers?
Find out what you can do with the domain	- Based on its status codes, can the domain be transferred to a different registrar? Can it be deleted or updated? - Which period in the domain life cycle is the domain currently at? Can anyone other than the previous registrant register the domain?

Details about a domain's infrastructure can significantly enrich cyber threat intelligence. Pivoting off these data points can help unearth a criminal domain infrastructure.

Contact Information

WHOIS records include the email addresses and phone numbers of the domain registrar, registrant, administrative, and technical contacts. What is the significance of these contact points? They are differentiated below.

- **Registrar:** The registrar oversees the administration of the domain. It has the power to transfer, delete, and renew the domain's registration at the registrant's request or when

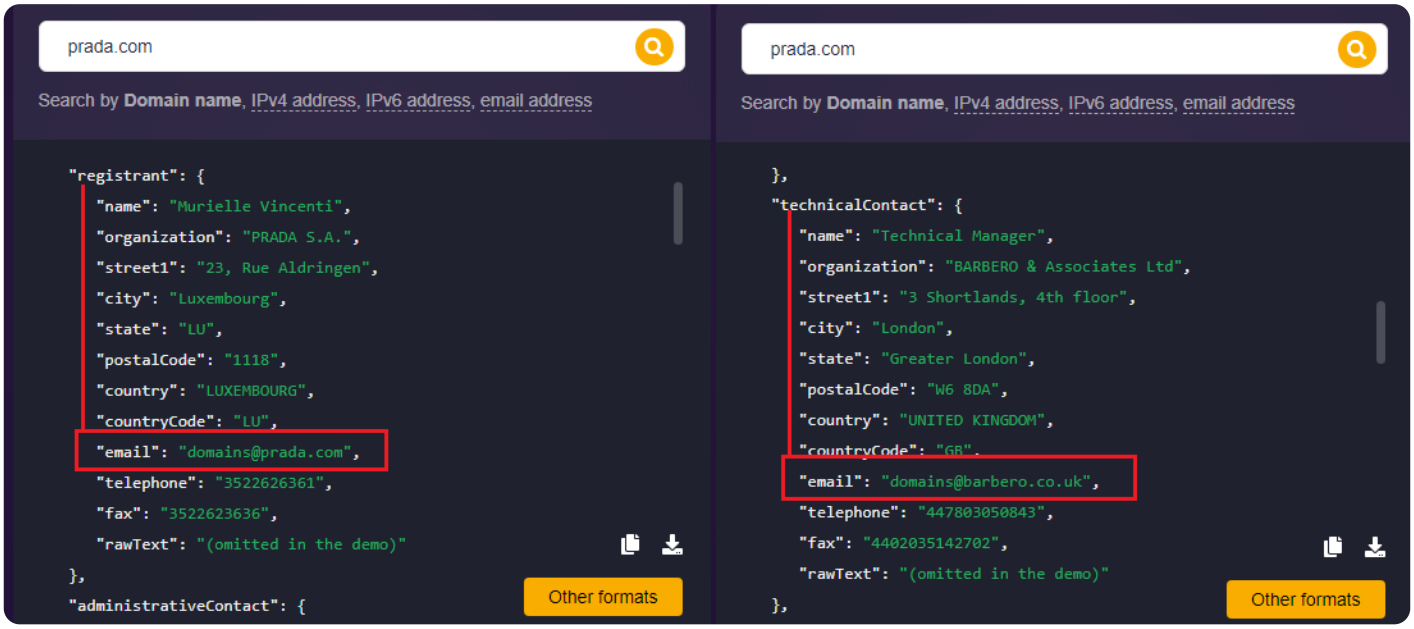
necessary, such as when the domain is reported for abuse. For this reason, the registrar's abuse contact email address is included in the domain's WHOIS record.

- **Registrant:** The registrant has direct control over the domain and is considered its owner.
- **Administrative contact:** The administrative contact information pertains to the person or department to get in touch with for billing concerns.
- **Technical contact:** The technical contact refers to the person or department responsible for maintaining and updating the domain's authoritative nameservers.

The administrative and technical contacts can also be separate companies, such as domain name management service providers.

These data points allow organizations to get in touch with people with a certain level of control over the domain. However, these contact details also have more subtle but essential uses that can help distinguish between legitimate and copycat entities.

For instance, thousands of Prada look-alike domains exist, but the legitimate Prada domain name (prada[.]com) uses the company's and domain manager's official email addresses. These are shown in the screenshots below.



On the other hand, look-alike or cybersquatting domains may have privacy-protected or mismatched contact email addresses. An example is pradausaonlinestore[.]com, whose WHOIS registrant email address doesn't match the official Prada registrant contact information.

```
  <rawText>Domain Name: pradausaonlinestore.com
Registry Domain ID: 2682223710_DOMAIN_COM-VRSN
Registrar WHOIS Server: grs-whois.aliyun.com
Registrar URL: http://www.alibabacloud.com
Updated Date: 2022-03-18T06:53:13Z
Creation Date: 2022-03-17T02:30:20Z
Registrar Registration Expiration Date: 2023-03-17T02:30:20Z
Registrar: ALIBABA.COM SINGAPORE E-COMMERCE PRIVATE LIMITED
Registrar IANA ID: 3775
Reseller:
Domain Status: ok https://icann.org/epp#ok
Registrant City:
Registrant State/Province: Kuala Lumpur
Registrant Country: MY
Registrant Email:https://whois.aliyun.com/whois/whoisForm
Registry Registrant ID: Not Available From Registry
Name Server: HAZEL.NS.CLOUDFLARE.COM
```

Below are some ways WHOIS contact information can help businesses, along with specific questions these data points can help answer.

Notable Use Cases	Description

Find out who has control over the domain	- Who is the domain's registrar? What are his or her contact details? - Who maintains and updates the domain's nameservers, as specified in the technical contact details?
Verify the contact details of a company	- What is the registrant's email address? Does it match any known legitimate contact information of the company associated with the domain? - Are the contact details redacted? Is this privacy redaction justifiable or consistent with other known domains of the company?
Facilitate the takedown of malicious or abused domains	- What are the registrant's contact details? How do you let the domain owner know if malicious subdomains have been added? - What are the registrar's abuse contact details?
Enrich business-to-business (B2B) contact lists	- What are the contact details of the companies in your target market? - For companies providing services and solutions to domain registrars, what are their contact details?

WHOIS contact information can help answer questions about a domain's ownership, administration, and credibility. They can fuel market intelligence and provide clues to help law enforcement agencies take down criminal infrastructure.

—

WHOIS data can answer straightforward questions, such as:

- How old is the domain?
- Who owns the domain, and how can they be contacted?
- What nameservers does the domain use?

These details can provide much-needed additional context to domain names for cybersecurity or business decision-making. WHOIS data can also become more powerful when combined with

other data points and intelligence sources, such as Domain Name System (DNS) databases, IP geolocation, malware detection engines, and phishing data repositories.

If you want to learn how we can provide real-time and historic access to massive WHOIS data, feel free to contact us or download our product sheet.