How to Trace a Privately Registered Domain’s Owner by Using a WHOIS History Lookup Tool

Posted on April 27, 2023

With a myriad of free readily available tools online, it’s not so difficult to find out if someone else already owns a domain you’re eyeing or if that domain is available for purchase or registration. But that’s where most tools stop. Sometimes, more details, such as a domain’s ownership history, including current and past registrants’ names and contact details, are hidden since most domain owners opt for privacy protection.

There are instances, though, when it's critical to obtain registrant information or find a hidden domain owner. For one, website owners who are interested in buying new domains need to know who to contact if someone already owns the domain they want to purchase. Another reason is when a domain of interest was used (typically misused or abused by cybercriminals) in attacks. In such cases, the domain's owner needs to be alerted to the situation for remediation. Finally, investigations launched by law enforcers or cybersecurity specialists may require more information on the domain registrant's identity.

These specific cases may require digging into a domain's WHOIS records. Problems arise, however, when pertinent details are not shown. For law enforcers who can subpoena for missing data, that may not be a problem. But for those who were victimized by attacks or turned into unwitting accomplices, that option might not be available. Specialized tools that obtain historical domain data might help there.

This post details how tools, such as WHOIS History Search, one of the nine tools that make up the Domain Research Suite (DRS), can help users uncover otherwise hidden registrant details without going through a potentially long and arduous legal channel.

Digging Deeper: The WHOIS History Search Advantage

We've come to know how crucial it can be to find out who is behind a domain that figured in a cyber attack. That helps researchers identify culprits and map an attack infrastructure so they can come up with solutions and future countermeasures. Without WHOIS information, they wouldn't usually know where to begin.

What others may not know, though, is that you can get relevant information from a historical WHOIS lookup tool. In fact, you may even get more. Tools, such as WHOIS History Search, give users data not only from a domain's current WHOIS record but also from all of its domain records since its creation. And so, if they can't get what they need from a current WHOIS record due to privacy protection, they can contact a domain of interest's last known registrant and start from there. In sum, it can not only be an alternative to a WHOIS lookup tool but an even better research partner.

The following list provides some of the many advantages of using a domain history lookup tool to

check a domain's owner.

It provides detailed information on all of a domain's past owners.

Users looking for a domain to use for their website are usually advised to get one that has been up for years. That is one way of lessening efforts to make it rank on search engine results pages (SERPs), which is crucial if you want to compete against tons of businesses that offer similar products or services. Then again, they'd also be warned about abandoned domains since the previous owners may have left them due to violations.

The question then is: How do you know which of the domains you're looking at is safe to purchase? That's where a WHOIS history lookup tool could come in handy. Run each domain you're interested in through the tool to find out every individual or company that has ever owned it. Once you have that list, check if any of them has had ties to malicious activity. You can do Google searches for registrant names, news sites, and the authorities who publicize cybercriminals' identities.

You can also check out publicly accessible blocklists, such as PhishTank. Run the domain through it to see if it has ever figured in a phishing attack. If you want to make sure that it isn't infringing on any trademarked brand, you can run it through the World Intellectual Property Organization (WIPO) database. Alternatively, you may rely on such tools as Domain Reputation API or Threat Intelligence Platform for a variety of useful investigations in a handy and integrated manner.

When it comes to choosing your business's "home," you can never be too careful. Keep in mind that any run-ins your domain has had in the past could affect your organization.

It can point you to a privately registered domain's current owner.

As we've said, if you're not from any law enforcement agency but need to get an idea on who's behind a domain without any red tape, you can get clues using a domain history lookup tool. How?

The Internet Corporation for Assigned Names and Numbers (ICANN) did not require WHOIS detail redaction until May 2018. As such, older domains (registered before then) are likely to have publicly available registrant information. Granted, these may or may not be the current owners, but for corporate domains, especially if their owners have been operating for some time, that is unlikely.

That said, if you're a cybersecurity specialist who wants to contact the owner of a domain used in an attack against your organization, you may contact its last known registrant. If the domain changed hands, its former owner might be able to point you to its new registrant.

It can help you build an attacker profile.

Let's face it: Most publications don't reveal all of an attack's indicators of compromise (IoCs), which could leave organizations open to attacks. One option for them would be to build their own attacker profiles using a historical domain lookup.

With a cybercriminal's name, you can run a reverse WHOIS lookup in combination with WHOIS History Search to gather all historical domain records. That will provide you with a list of all domains (past and present) containing the attacker's name. You can then screen these domains, and those that are proven malicious or connected to the cybercriminal can be blocked.

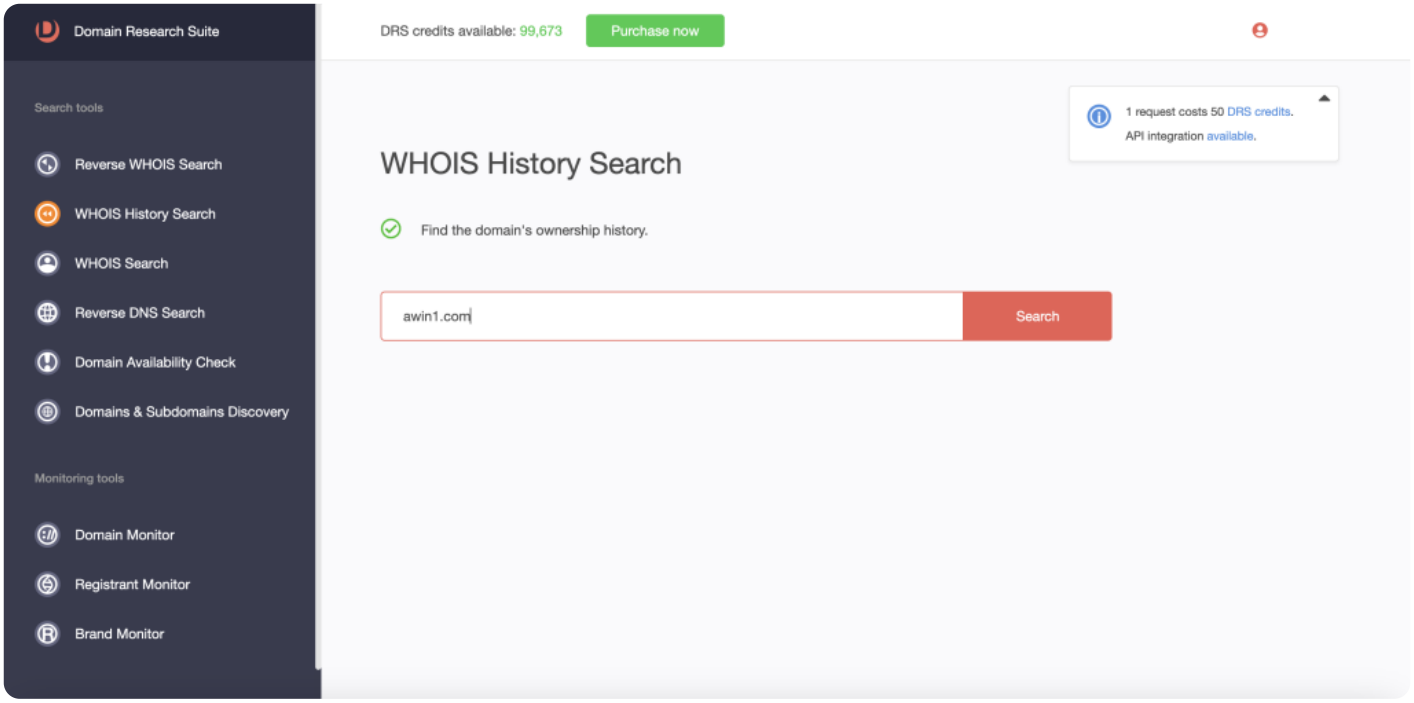
How to Find Out Who Owns a Private Domain

Here's a step-by-step guide on using WHOIS History Search on a privacy-protected domain of

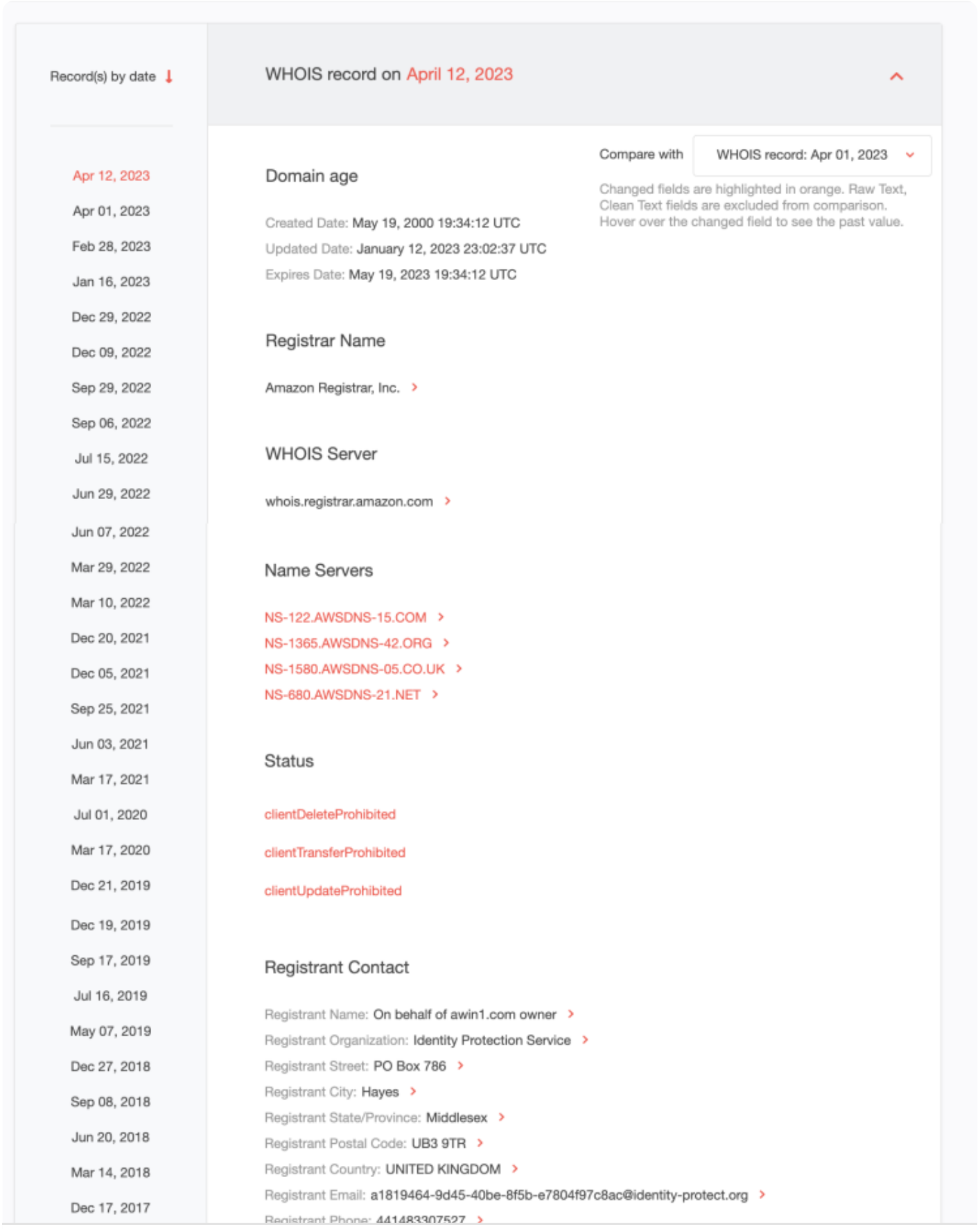
interest.Access the WHOIS History Search dashboard at https://tools.whoisxmlapi.com/whois-history-search.

1. Access the WHOIS History Search dashboard at https://tools.whoisxmlapi.com/whois-history-search.

2. Type the domain name into the search input field then click Search. For this demonstration, we used an IoC for a business email compromise (BEC) attack.



3. Its current WHOIS record dated April 12, 2023 shows it is privacy-protected.


Record(s) by date
Apr 12, 2023
Apr 01, 2023
Feb 28, 2023
Jan 16, 2023
Dec 29, 2022
Dec 09, 2022
Sep 29, 2022
Sep 06, 2022
Jul 15, 2022
Jun 29, 2022
Jun 07, 2022
Mar 29, 2022
Mar 10, 2022
Dec 20, 2021
Dec 05, 2021
Sep 25, 2021
Jun 03, 2021
Mar 17, 2021
Jul 01, 2020
Mar 17, 2020
Dec 21, 2019
Dec 19, 2019
Sep 17, 2019
Jul 16, 2019
May 07, 2019
Dec 27, 2018
Sep 08, 2018
Jun 20, 2018
Mar 14, 2018
Dec 17, 2017
WHOIS record on April 12, 2023
Compare with
WHOIS record: Apr 01, 2023
Changed fields are highlighted in orange. Raw Text, Clean Text fields are excluded from comparison. Hover over the changed field to see the past value.
Domain age
Created Date: May 19, 2000 19:34:12 UTC
Updated Date: January 12, 2023 23:02:37 UTC
Expires Date: May 19, 2023 19:34:12 UTC
Registrar Name
Amazon Registrar, Inc.
WHOIS Server
whois.registrar.amazon.com
Name Servers
NS-122.AWSDNS-15.COM
NS-1365.AWSDNS-42.ORG
NS-1580.AWSDNS-05.CO.UK
NS-680.AWSDNS-21.NET
Status
clientDeleteProhibited
clientTransferProhibited
clientUpdateProhibited
Registrant Contact
Registrant Name: On behalf of awin1.com owner
Registrant Organization: Identity Protection Service
Registrant Street: PO Box 786
Registrant City: Hayes
Registrant State/Province: Middlesex
Registrant Postal Code: UB3 9TR
Registrant Country: UNITED KINGDOM
Registrant Email: a1819464-9d45-40be-8f5b-e7804f97c8ac@identity-protect.org
Registrant Phone: 441483307527

4. Look at the next records arranged from newest to oldest until you find one with public registrant details. In this domain's case, that would be the WHOIS record for October 15, 2016.

WHOIS record on October 15, 2016

Compare with WHOIS record: May 08, 2016

Changed fields are highlighted in orange. Raw Text, Clean Text fields are excluded from comparison. Hover over the changed field to see the past value.

Domain age

Created Date: May 19, 2000 00:00:00 UTC

Updated Date: April 20, 2016 00:00:00 UTC

Expires Date: May 19, 2017 00:00:00 UTC

Registrar Name

TUCOWS DOMAINS INC.

WHOIS Server

whois.tucows.com

Name Servers

NS-1138.AWSDNS-14.ORG|NS-1733.AWSDNS-24.CO.UK|NS-316.AWSDNS-39.COM|NS-991.AWSDNS-59.NET|

Status

ok

https://icann.org/epp#ok

Registrant Contact

Registrant Name: Peter Loveday

Registrant Organization: ZANOX AG

5. You can contact the domain’s past owner who may know its current registrant.

Try your hand at tracking down the owner of a privately registered domain now with WHOIS History Search via the Domain Research Suite (DRS). Access your account or try it for free.