How to Retrieve Domain WHOIS History Data After Redaction

Posted on March 29, 2023

WHOIS information is indispensable for any cybersecurity researcher. It is an essential resource for tracking down registration owners for a variety of reasons that range from settling trademark and cybersquatting disputes to configuring websites. With WHOIS records, a security analyst or website administrator can quickly get in touch with a registrant owner to resolve or file a dispute, transfer a domain with ease, or set up a valid Secure Sockets Layer (SSL) certificate.

With the General Data Protection Regulation (GDPR) implementation, however, the Internet Corporation for Assigned Names and Numbers (ICANN) was compelled to modify its policies for WHOIS data availability. ICANN’s implementation of the Temporary Specification for Generic Top-Level Domain (gTLD) Registration Data in 2018 resulted in the redaction of millions of WHOIS records from the public domain.


Binder
Binder
Binder
Binder

Under the new rule, both registrars and registries must explicitly state that a domain's ownership details have been "Redacted for Privacy," unless, of course, the domain owner consents to share his or her registrant information publicly. This policy applies to all data accessible via WHOIS or Registration Data Access Protocol (RDAP) protocols.

WHOIS lookups have become more complicated ever since. What was once an activity that took a couple of minutes, now involves hours of Internet research and hopping from one application or database to another. Fortunately, there are other ways listed below through which analysts can obtain this critical domain data, such as a WHOIS history search tool.

What Are the Alternatives?

GDPR doesn't necessarily spell the end for publicly available WHOIS information, though. The temporary specification still allows users to obtain WHOIS data from registry operators for legitimate reasons by filing a request. Requesting parties must be able to prove that the domain has been engaged in cybersquatting, fraud, and other illegal activities. While the request process comes with its own set of challenges (i.e., lack of standardization for filing steps), there's no reason why security researchers should not pursue it.

For urgent requests, such as in the event of a criminal investigation, users can file for a subpoena. Subpoenas may cost users more and may take time, but it is the fastest route for requesting parties who hit a dead end with their WHOIS platforms or have not received any response from registrars. Some registrars may sometimes not respond to such requests for fear of violating GDPR.

Another means for cybersecurity researchers to get a domain's registrant record is by requesting it from abuse contacts. Registrars had to put up an abuse contact email for a domain in compliance with GDPR.

How WHOIS History Search Can Help

Domain researchers can rely on WHOIS History Search when they encounter privacy-protected WHOIS details, especially for offending domains. By retrieving a domain's last known registrant details, it's possible to learn more about a domain's past usage and affiliations.

WHOIS History Search is part of our nine-in-one suite of domain monitoring and search tools, Domain Research Suite (DRS). It enables users to find a domain's historical records. These are segregated by date when the domain received updates and drawn from a comprehensive database that encompasses 15.6B+ domains that our company has crawled for over ten years. That explains why the tool yields accurate and complete results for domains.

Below are some common use cases of the tool.

- **Combating fraud:** WHOIS History Search can be used to collect evidence on fraudulent domains or infringers for trademark disputes, lawsuits, and cyber investigations.
- **Tracking attackers:** The tool can find associations between suspicious domains and known cybercriminal networks.
- **Domain investing:** Domainers can use it to determine whether a domain is a worthy investment and if it has no ties to any malicious campaigns.

Steps in Retrieving Domain History Data

- Sign up for an account on the Domain Research Suite landing page. Each new account comes with 500 free DRS credits.
- Enter a domain name into the WHOIS History Search dashboard.

- The tool displays all historical WHOIS records for it, including its creation and expiration dates, current and previous owners and registrars, status, contact details, and name and WHOIS servers. The results fall into two sections:
    - The first section includes a tally of how many WHOIS records the domain has, the number of detected changes, registrars, records with public ownership data, and the total number of days the domain has been active.
    - The second section includes a breakdown of the records by date and expands the results to view each record.

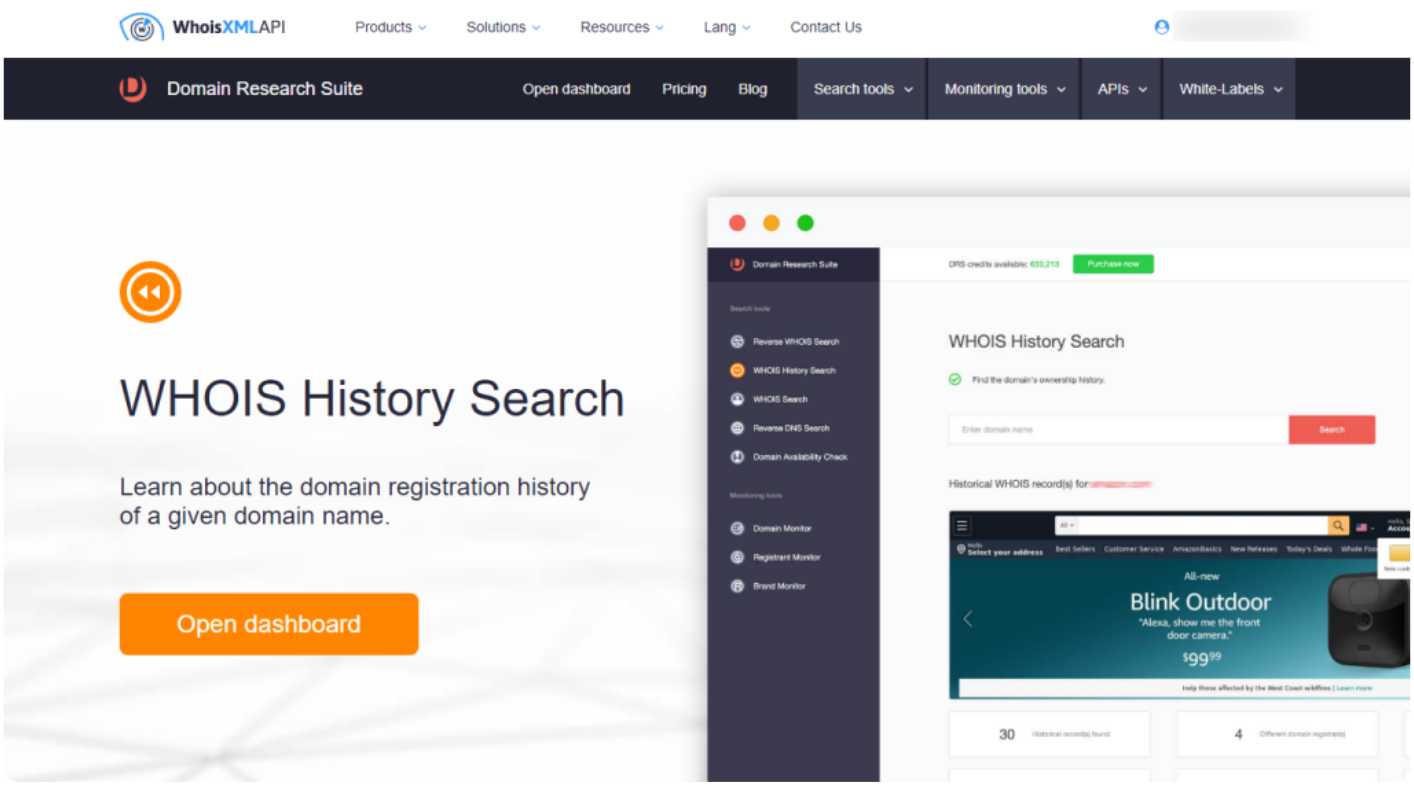
- Users can download the results to their computers in the form of a PDF file. Alternatively, if they prefer a command-line tool similar to the original “whois” command to find the required records, this service can also be used with our “bestwhois” command-line tool after the subscription.

You may also like: Who is History Search Web Tool Tutorial

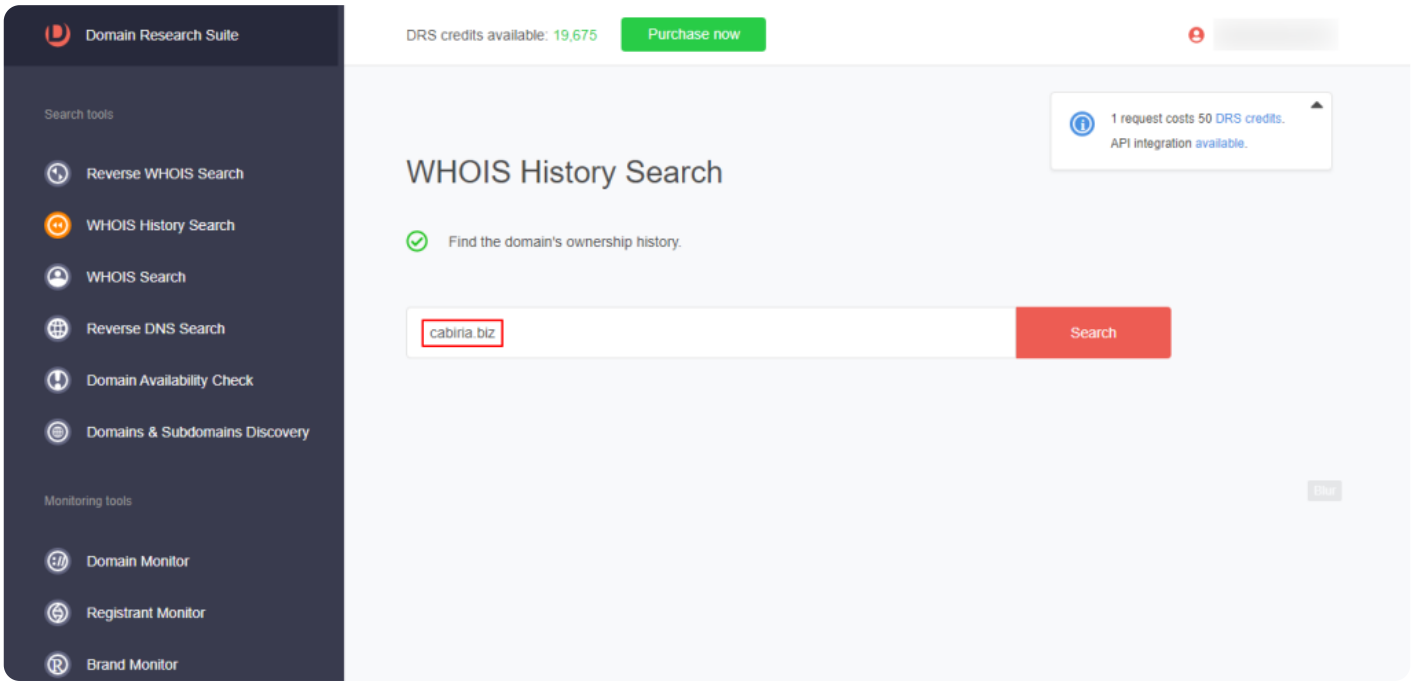
WHOIS History Search Demo for Retrieving Unredacted Record Details of an Attack IoC

It’s not uncommon for cybersecurity researchers to stumble upon domains identified as indicators of compromise (IoCs) whose WHOIS records have been GDPR-masked. If that’s the case, they can follow this step-by-step guide to go on with their investigation.

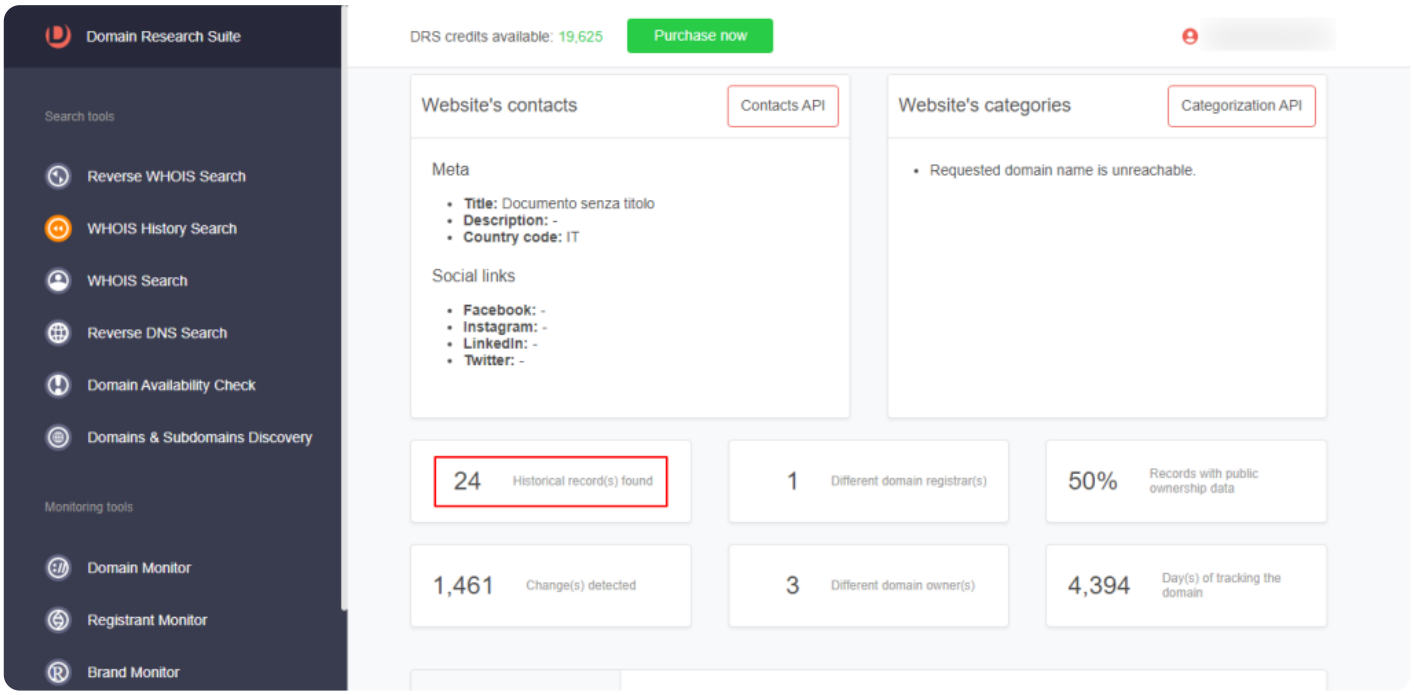
1. Go to the WHOIS History Search website https://drs.whoisxmlapi.com/whois-history. Log in.



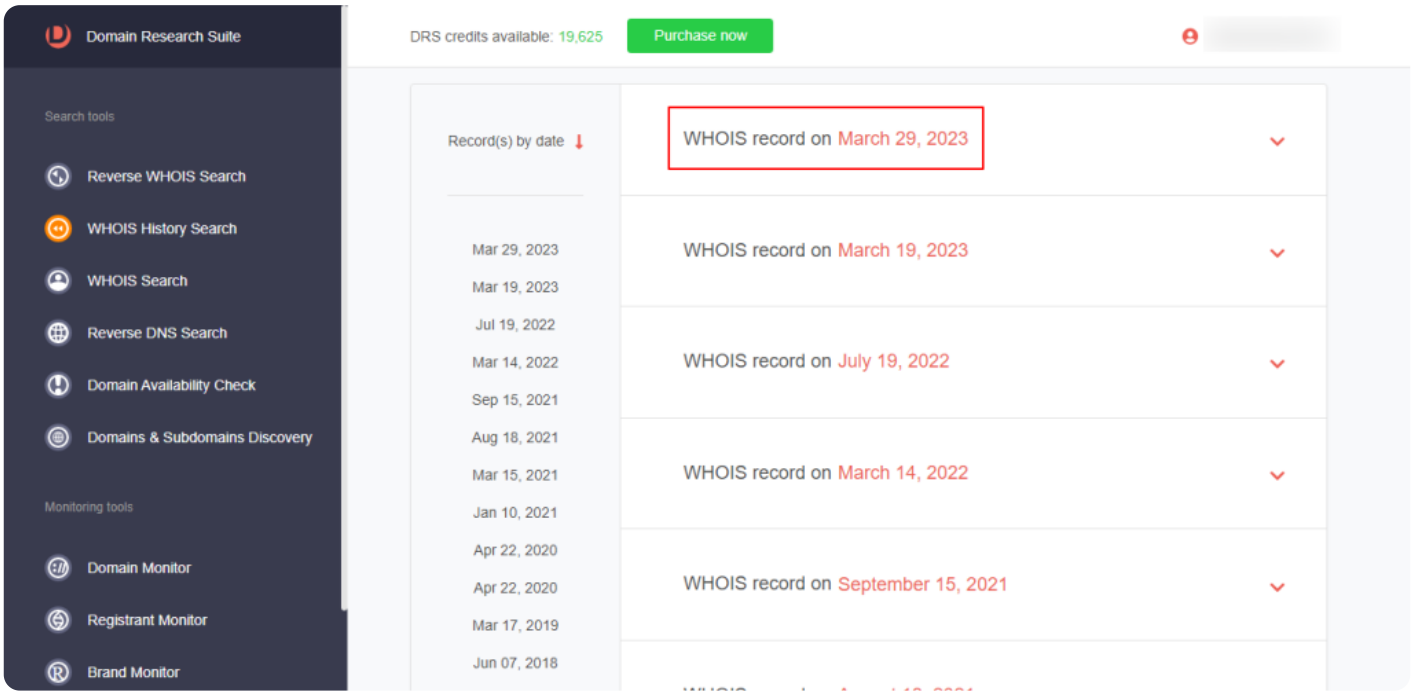
2. Type the domain name you want to investigate into the Search input field then click **Search**. For this demonstration, we used cabiria[.]biz—a known Lorec53 IoC.



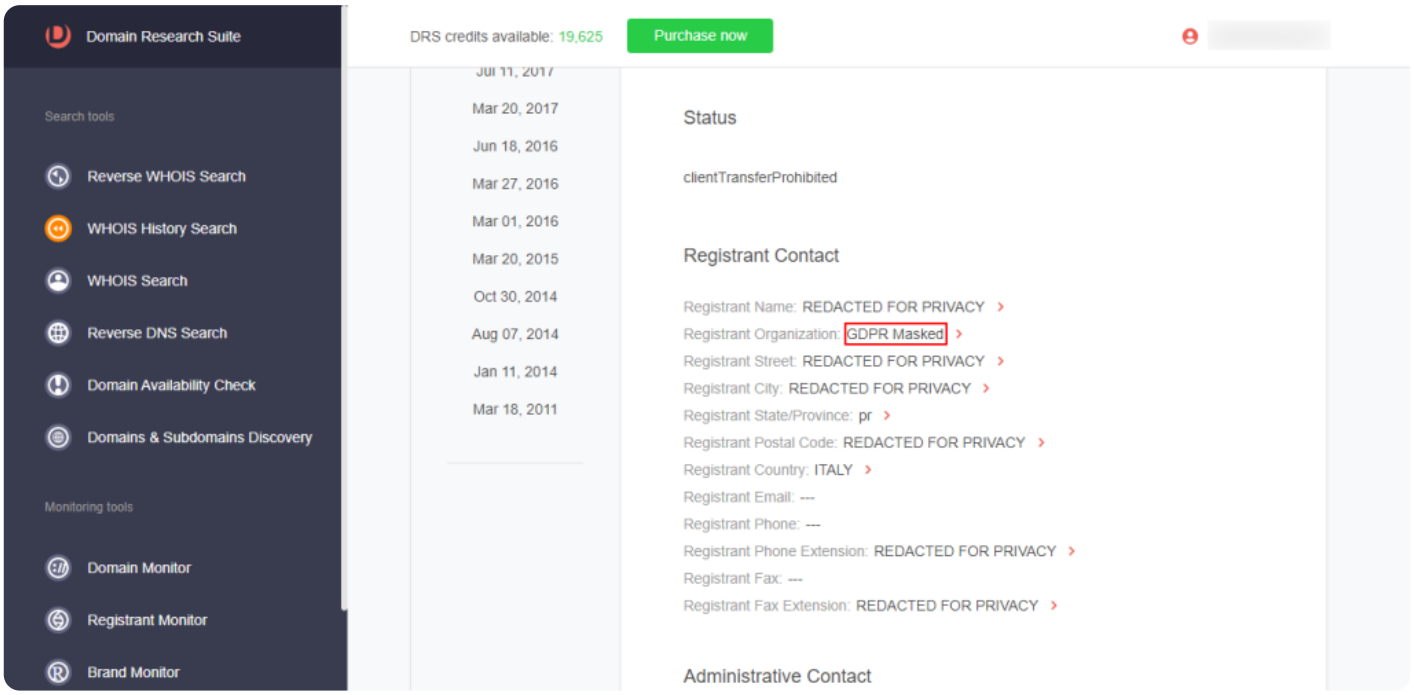
3. Scroll down to see how many historical WHOIS records the domain has. The bigger the number, the more chances you'll have of finding out who may own it.



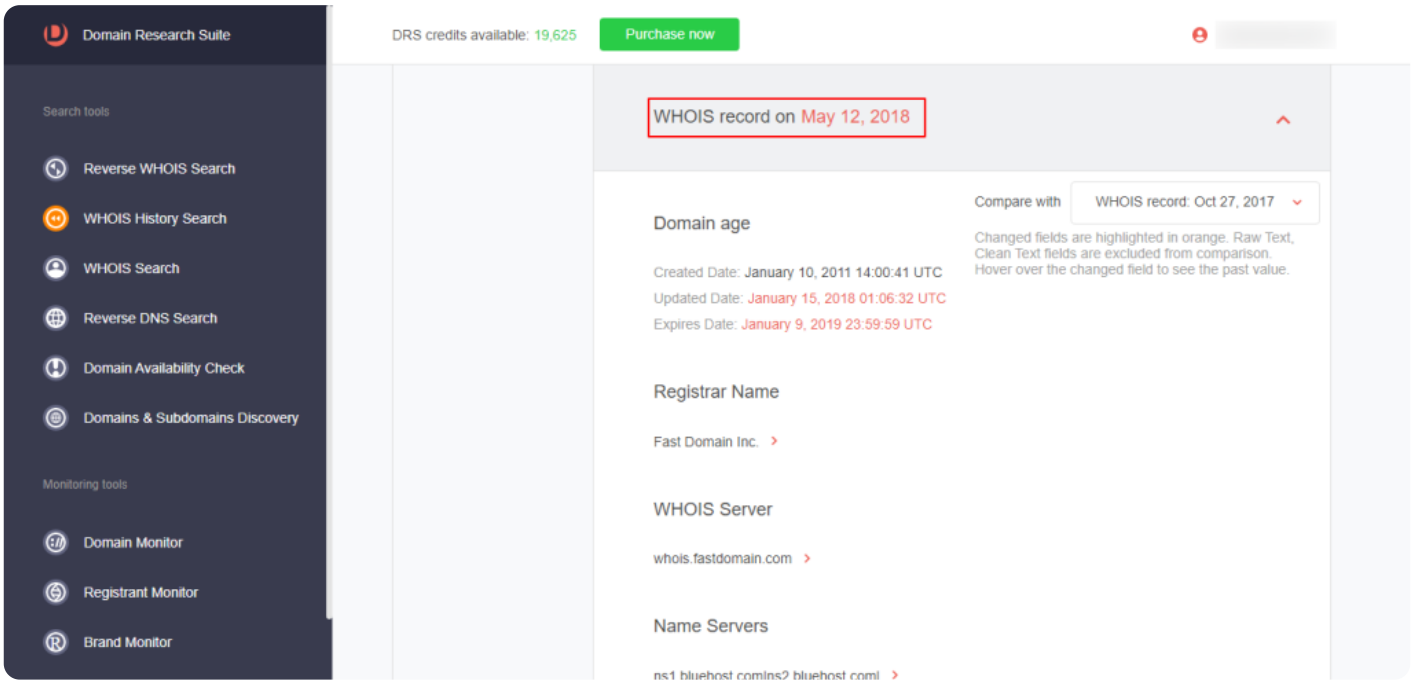
4. Open the domain's current WHOIS record. In this case, that would be the one at the top dated March 29, 2023.



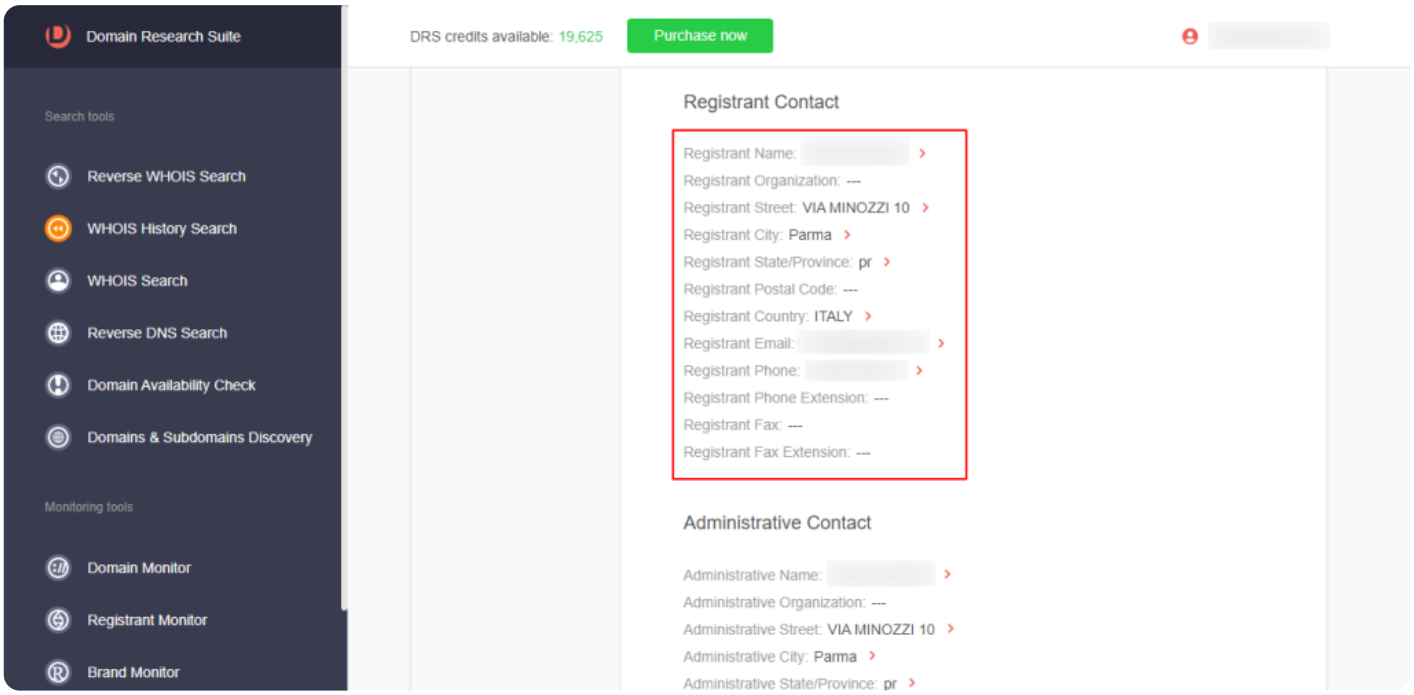
5. Scroll down to see if the record's registrant details are public. In this case, they've been GDPR-masked.



6. Open all available historical WHOIS records until you see one whose registrant details haven't been redacted. In this case, that would be the one dated May 12, 2018.



7. Scrolling down the record would give you the domain's owner's name, email address, phone number, and other details. We've redacted them here for privacy reasons. If you're a security researcher, you can use the information to find other Lorec53 artifacts.



GDPR has undoubtedly impacted users who need to access WHOIS data for research purposes. Despite hurdles, however, WHOIS History Search empowers cybersecurity researchers, domainers, marketing professionals, and website developers to get hold of a domain's WHOIS history and, thus, push on with their efforts in some cases. Due to its database's breadth, WHOIS History Search is capable of acquiring complete and accurate WHOIS records for any domain that has been online before GDPR implementation.