How to Retrieve Domain WHOIS History Data After Redaction

Posted on March 24, 2026

WHOIS data is useful for tracking down cyber threats, verifying business ownership, and preventing domain brand abuse. For decades, this information was public and easy to access.

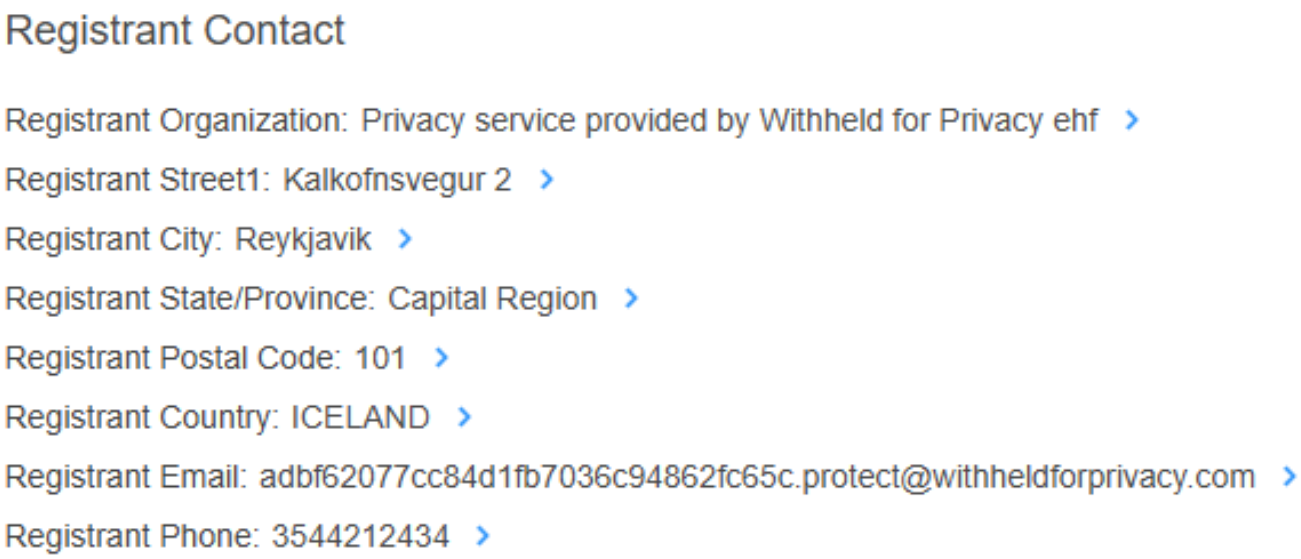
Lately, finding the person behind a domain name has become much harder. A regular WHOIS lookup provides very little, as most information is now either redacted or privacy-protected (these are different mechanisms that we'll get into later).

In this post, we'll describe some ways cybersecurity researchers can still get access to real WHOIS information despite the redaction or privacy protection. We will also talk about why WHOIS data is now protected.

WHOIS Redaction vs. WHOIS Privacy

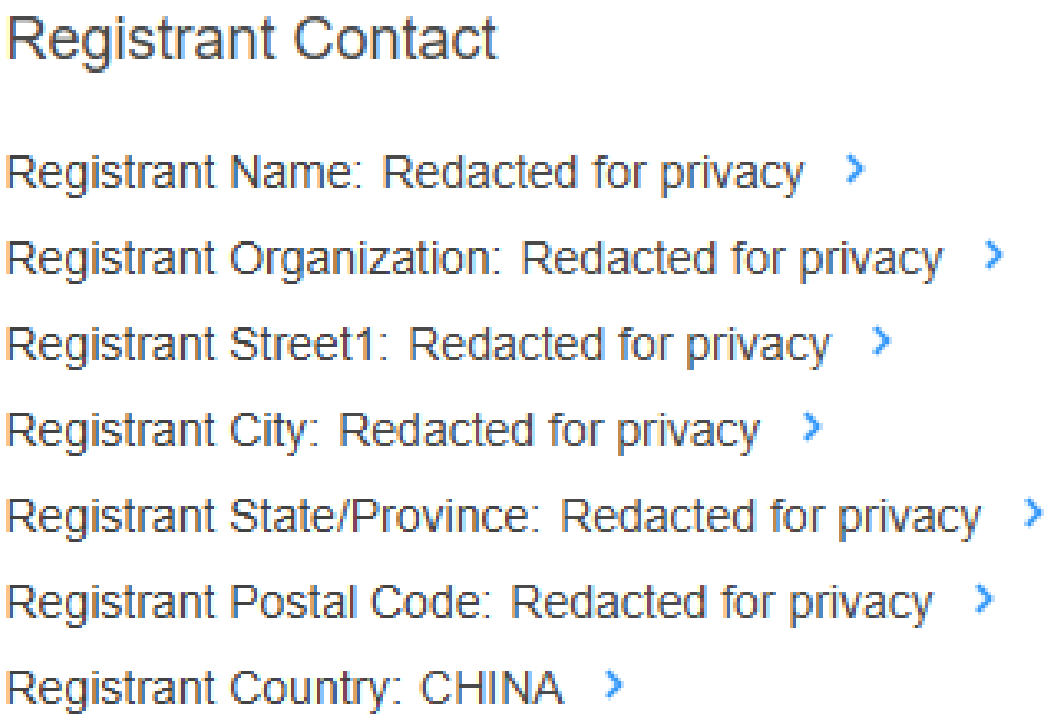
WHOIS redaction and WHOIS privacy may sound like the same thing, and to some extent, it's true — they both hide registrant information. However, they work differently.

WHOIS privacy is a service — in some cases, you need to actually pay for it. These services work with domain registrars and replace your personal information with proxy domain contact details. If someone looks up a domain with privacy protection, they see "Withheld for privacy," "Domains by Proxy," or the name and address of some other WHOIS privacy service provider, but not the actual domain owner.



Example: Registrant details of flosspols[.]org show "Withheld for Privacy ehf" instead of the owner's contact details

WHOIS redaction is different. It is not a choice made by the user, but a policy enforced by the registrar or registry. Redaction removes the information entirely from public view. Instead of seeing a proxy name, you see a label like "Redacted for Privacy."



Example: Registrant details of housedmd[.]com — most of the WHOIS record is redacted for privacy

Why Is WHOIS Redacted for Privacy?

While WHOIS privacy services have been around for decades (for example, Domains by Proxy was founded in 2004), redaction only started with the onset of the General Data Protection Regulation (GDPR). When GDPR took effect in Europe, the Internet Corporation for Assigned Names and Numbers (ICANN) had to change how it handled registration data.

In 2018, ICANN implemented the Temporary Specification for Generic Top-Level Domain (gTLD) Registration Data. This rule required domain registrars and registries to hide personal data unless

the domain name owner explicitly consented to its disclosure. This policy applies to all gTLD data accessible via standard WHOIS or the newer Registration Data Access Protocol (RDAP). While ccTLDs are governed independently, many still chose to follow ICANN's lead.

WHOIS lookups have become more complicated ever since.

Previously, getting a domain owner's email took seconds and required one regular WHOIS lookup — whether using a WHOIS lookup tool like ours or the whois command. After redaction, in many cases, WHOIS lookups don't give you much value. Where real owner data used to be, you keep seeing placeholder emails from WHOIS privacy protection services (that actually work for contacting the owner, but are completely useless for reverse WHOIS or other purposes) or fields that simply say "Withheld for Privacy" or "Redacted for Privacy." While this does protect the owners' privacy, it also creates a lot of cybersecurity problems.

Is All WHOIS Data Redacted?

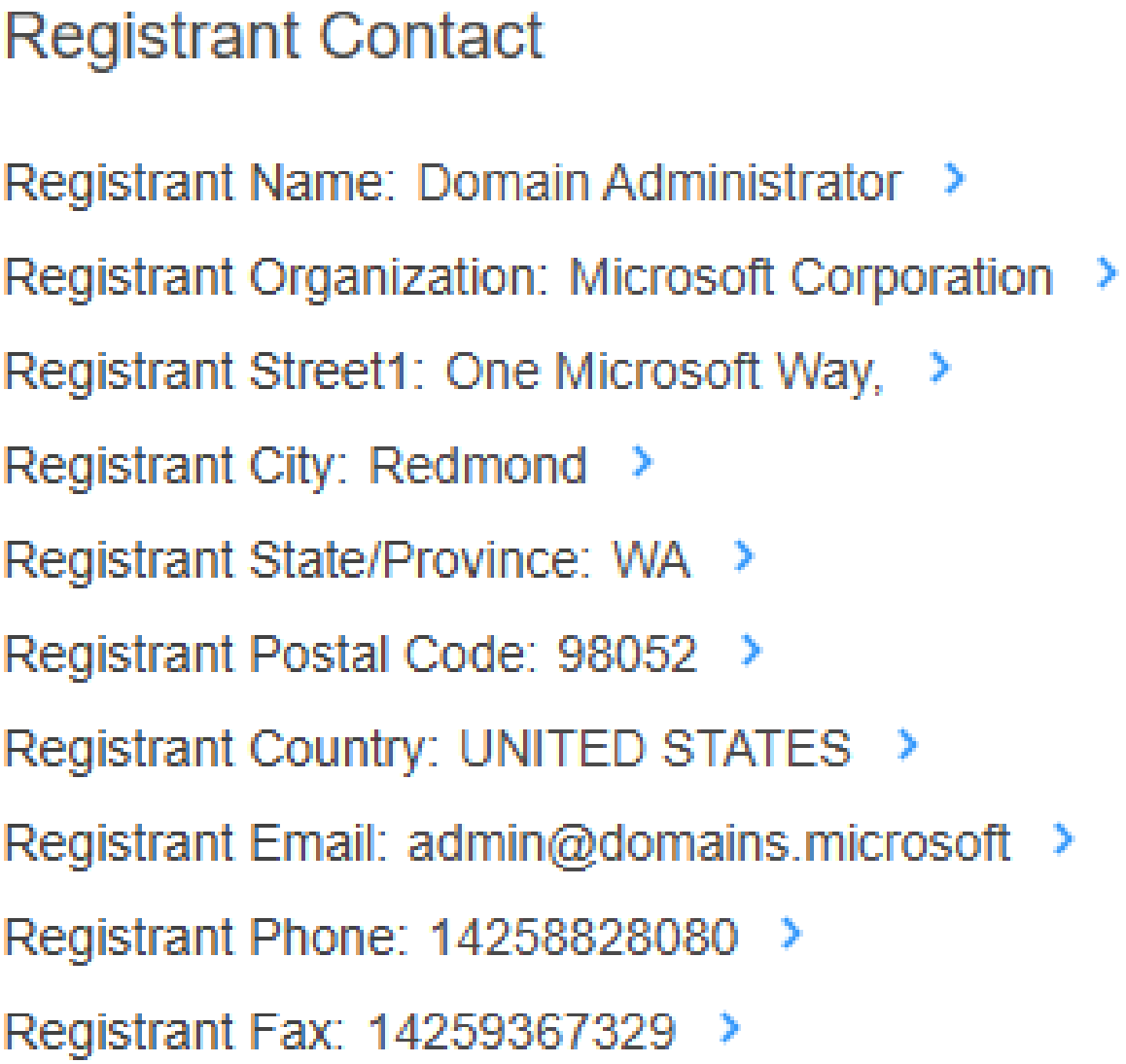
Fortunately, not every domain registration record is redacted. Here are some instances when WHOIS is not redacted or hidden by WHOIS privacy:

- **Pre-2018 WHOIS data**: While many domains registered before 2018 have "REDACTED" across most of their current WHOIS record fields, they also have historical records that used to be public and were not redacted back then. That old data is likely still accessible via historical archives such as our WHOIS History Database Download. If the domain did not change hands or the owner didn't change their contact details, this information may be a goldmine for those looking for the owner's details. However, domain owners who used WHOIS privacy services before 2018 would still have hidden WHOIS records for their domains.

- **Domains sporting some country-code top-level domains (ccTLDs)**: Some ccTLDs have unredacted WHOIS information since the registries don't allow redaction (as per the

respective countries' laws). Examples include Australia (.au, at least for the registry's web-based WHOIS lookup tool), Niue (.nu), and the United States (.us, although there's a proposal to change this).

- **Domains where owners chose to explicitly show their WHOIS data**: In many cases, the domain registrant has the freedom to publicly show their WHOIS record if they want to. Bigger enterprises, such as Microsoft, for example, use WHOIS as a trust signal, showing that a domain really belongs to them rather than to some impersonators.



Current registrant contact details for microsoft[.]com

Which WHOIS Data Is Redacted?

Redacted WHOIS information includes personal data, such as the registrant name, organization, email address, and postal address.

However, technical data about the domain remains public. This includes nameservers, domain status codes, dates, registrant state/province, and registrant country.

Data Field	Redacted?
Registrant name	Yes
Registrant email	Yes
Postal address	Yes
Registrant organization	Yes
Nameservers	No
Creation and expiration dates	No
Registrant country	No (usually)
Domain status codes	No

The data that is left unredacted is considered to not be personal, so GDPR allows for it to stay public.

How To Access Redacted Registrant and Other WHOIS Data

You have a few options if you really need to find the person behind redacted WHOIS information. These range from filing formal requests to using specialized historical databases.

File a Disclosure Request

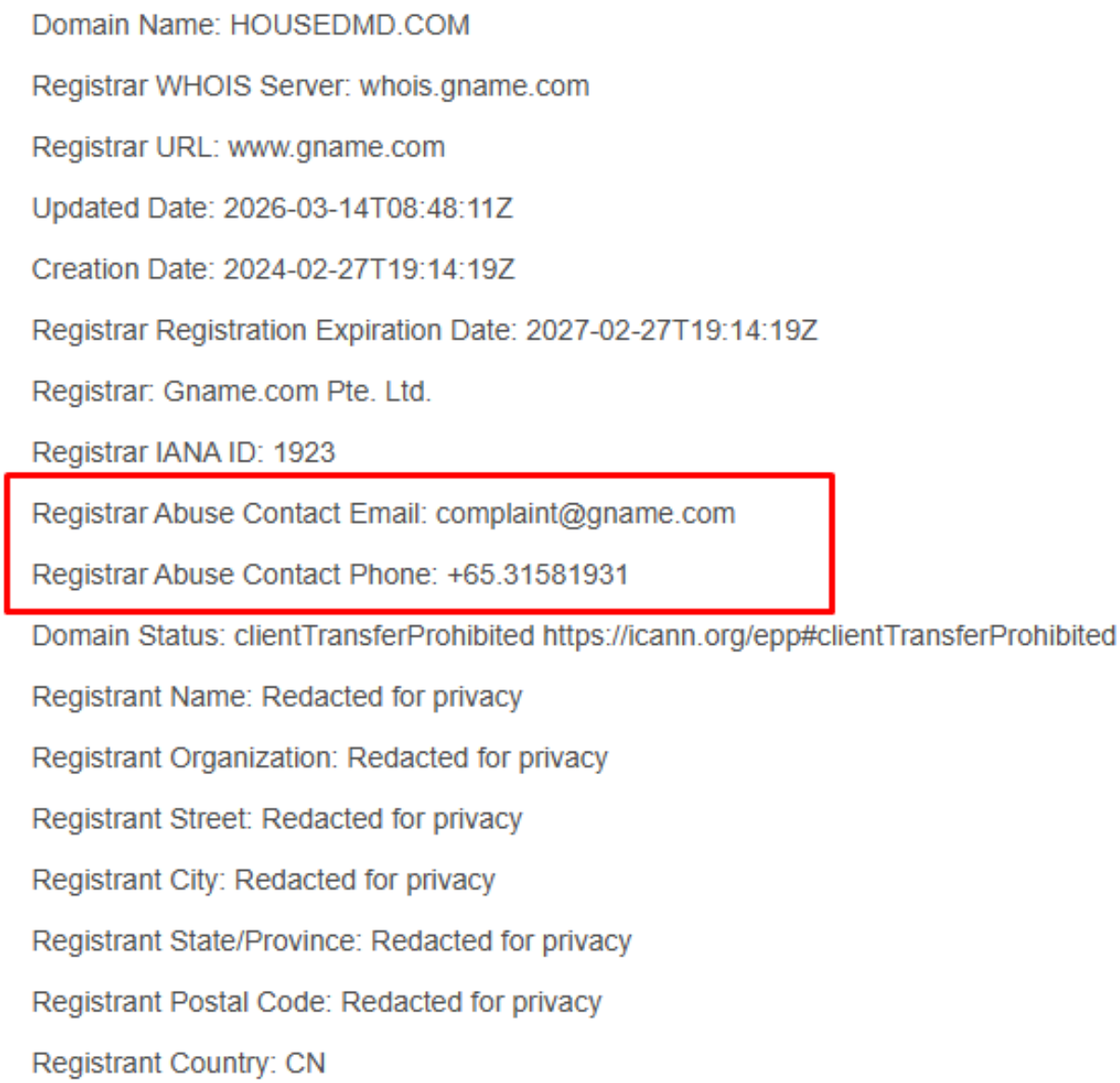
GDPR allows domain registries to share registration data as long as the request is for legitimate reasons.

Cybersecurity researchers can file a request with the registrar for domains involved in illegal activities, such as fraud, cybersquatting, or phishing. There’s no standard anti-abuse system for filing these requests, as domain name registrars have their own processes.

Some examples are:

- GoDaddy: Uses its own non-public data disclosure form.
- OVH: Its procedure is detailed here, and requests should be sent to domain-disputes@ovh.net.
- Cloudflare: Handles these requests through their abuse reporting system.
- Namecheap: Provides different processes for different purposes, which they detail in this guide.

There is also an "Abuse Contact" listed in the redacted WHOIS record, since registrars are required to provide a way to report abuse even if the owner's personal data is hidden. It’s usually found after the registrar's name and ID.



Domain Name: HOUSEDMD.COM
Registrar WHOIS Server: whois.gname.com
Registrar URL: www.gname.com
Updated Date: 2026-03-14T08:48:11Z
Creation Date: 2024-02-27T19:14:19Z
Registrar Registration Expiration Date: 2027-02-27T19:14:19Z
Registrar: Gname.com Pte. Ltd.
Registrar IANA ID: 1923
Registrar Abuse Contact Email: complaint@gname.com
Registrar Abuse Contact Phone: +65.31581931
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Name: Redacted for privacy
Registrant Organization: Redacted for privacy
Registrant Street: Redacted for privacy
Registrant City: Redacted for privacy
Registrant State/Province: Redacted for privacy
Registrant Postal Code: Redacted for privacy
Registrant Country: CN

Example: Registrar abuse information for housedmd[.]com

File and Then Serve a Subpoena

For criminal investigations, the most fruitful route to take is filing a subpoena. It costs more and

requires legal counsel, but it is often the only way to get a response from a registrar. If a registrar receives a valid legal order, they are generally required to hand over the unredacted registrant information.

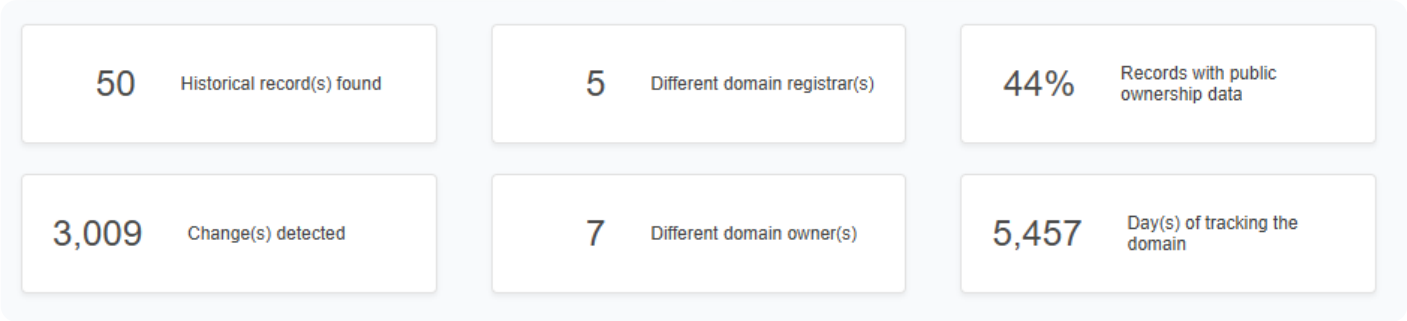
The FBI, for one, has subpoenaed many registrars. In 2025, they served one to Tucows in their effort to track down the owner of archive[.]today, archive[.]is, and archive[.]ph.

Use WHOIS History

The quickest and easiest method is using historical WHOIS data. It allows cybersecurity researchers to find out what the WHOIS records looked like before redaction was applied. For example, if a domain name was registered in 2015 and redacted in 2018, the historical records from those first three years could be a gold mine (provided the domain owner didn't use WHOIS privacy services).

Below, we'll show you how to use WHOIS History Search, part of Domain Research Suite (DRS), a platform that has 10 domain search and monitoring tools:

1. **Log in to DRS.** If you don't have an account yet, sign up for free and get 500 free credits.
2. **Enter the domain name.** For example, if you are investigating xclyd[.]com, a domain tagged as a Silver Fox indicator of compromise (IoC), type it into the search field.
3. **Check the record count.** A high number of historical records increases your chances of finding an unredacted version.



Summary of WHOIS record changes for xclyd[.]com spanning across 14+ years.

4. **Open the domain's current WHOIS record.** In this case, that would be the one at the top, dated March 19, 2026, which is already redacted for privacy across its registrant, administrative, and technical contacts.

Registrant Contact

Registrant Name: Redacted for privacy
Registrant Organization: Redacted for privacy
Registrant Street: Redacted for privacy
Registrant City: Redacted for privacy
Registrant State/Province: Redacted for privacy
Registrant Postal Code: Redacted for privacy
Registrant Country: UNITED STATES
Registrant Email: ---
Registrant Phone: ---
Registrant Phone Extension: ---
Registrant Fax: ---
Registrant Fax Extension: ---

Redacted registrant contact details of xclyd[.]com dated March 19, 2026.

5. **Look for older records.** Scroll back to records dated before May 2018. The oldest record for xclyd[.]com is dated April 10, 2011, and it shows an unredacted registrant organization, name, email address, and postal address for the domain's administrative, technical, and billing contact.

Registrant Contact

Registrant Name: ZhiJian Peng
Registrant Organization: HUI CONG
Registrant Street: Beijing
Registrant City: Beijing
Registrant State/Province: Beijing
Registrant Postal Code: [redacted]32
Registrant Country: CHINA
Registrant Email: ---
Registrant Phone: ---
Registrant Phone Extension: ---
Registrant Fax: ---
Registrant Fax Extension: ---

Administrative Contact

Administrative Name: ZhiJian Peng
Administrative Organization: ZhiJian Peng

Oldest registrant and administrative contact information of xclyd[.]com dated April 10, 2011.

The most recent unredacted WHOIS record for the domain is dated April 4, 2018. After that, the details were hidden. However, we can still see that the domain remained registered in China until February 1, 2026.

Registrant Contact

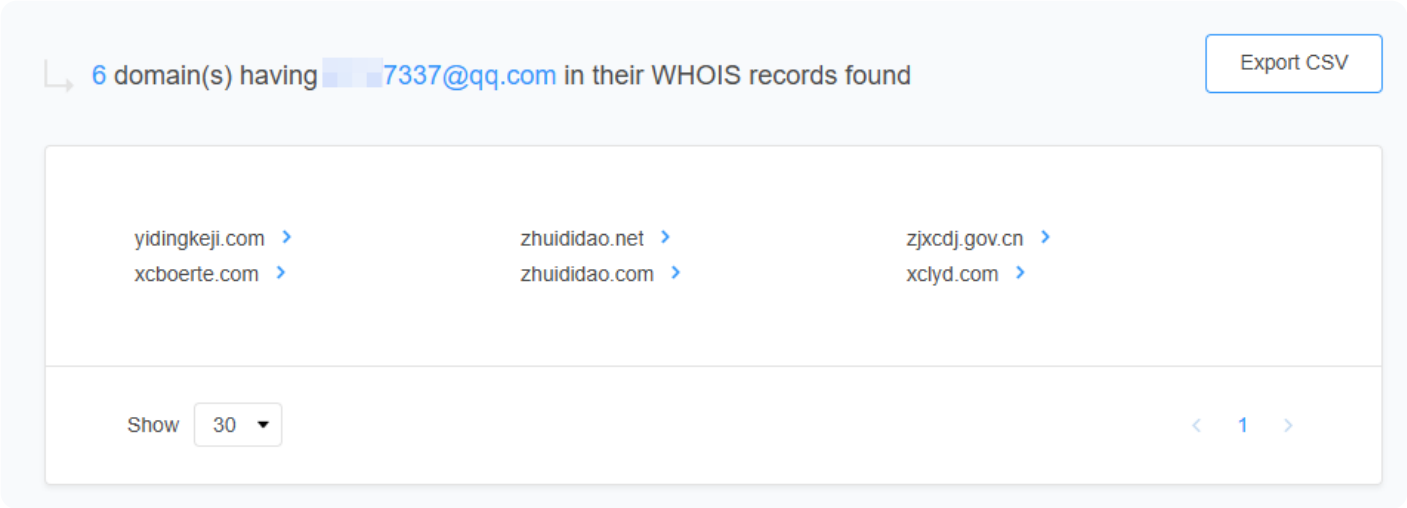
Registrant Name: Yong Da
Registrant Organization: Zhe Jiang Li Yong Da Zhi Ling Ji Xie You Xian Gong Si
Registrant Street: Xin Chang Cheng Dong Xin Qu Yu Lin Lu 18Hao
Registrant City: Shao Xing Shi
Registrant State/Province: Zhe Jiang
Registrant Postal Code: 500
Registrant Country: CHINA
Registrant Email: 7337@qq.com
Registrant Phone: 86041483
Registrant Phone Extension: ---
Registrant Fax: 586041483
Registrant Fax Extension: ---

Administrative Contact

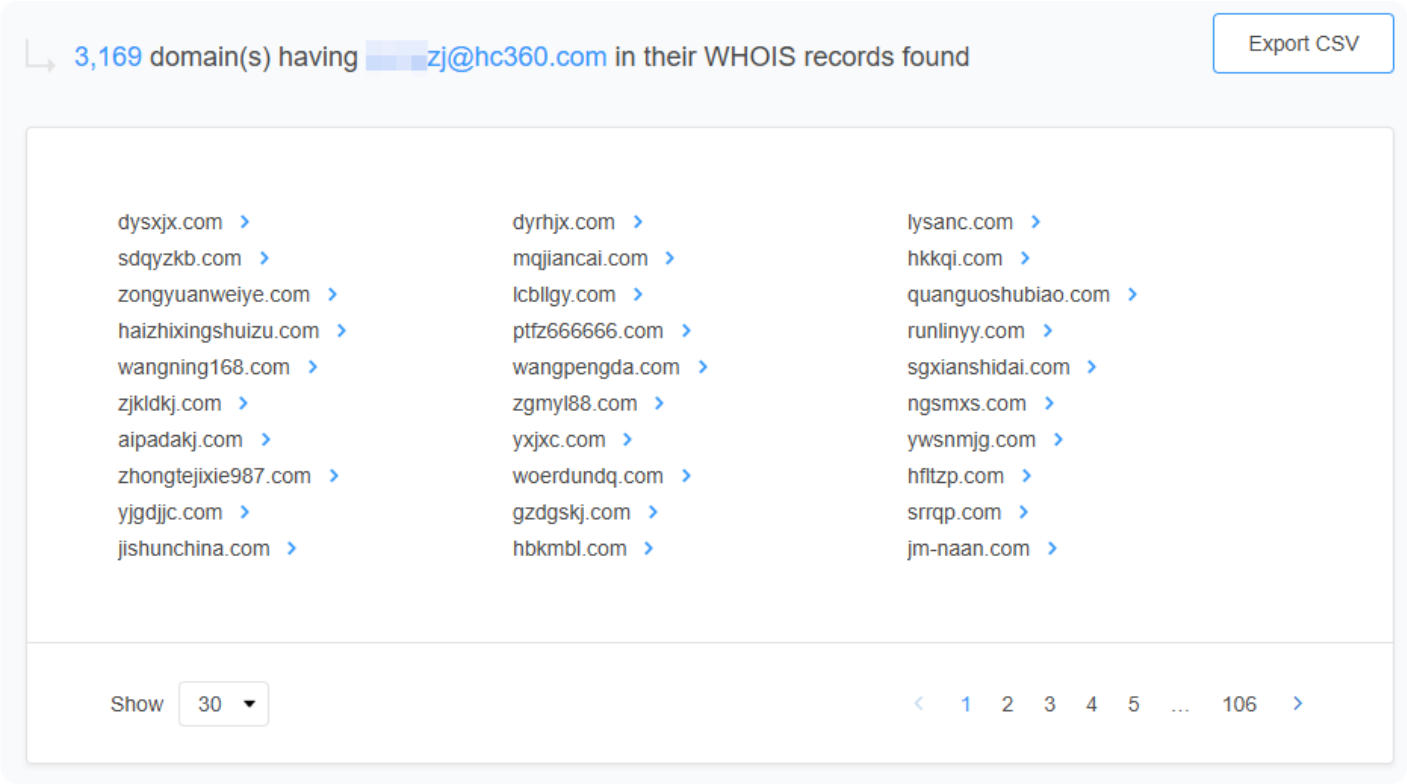
Administrative Name: Yong Da
Administrative Organization: Xin Chang Xian Li Yong Da Zhi Ling Ji Xie You Xian Gong Si
Administrative Street: Xin Chang Cheng Dong Xin Qu Yu Lin Lu 18Hao
Administrative City: Shao Xing Shi
Administrative State/Province: Zhe Jiang
Administrative Postal Code: 500
Administrative Country: CHINA
Administrative Email: 7337@qq.com
Administrative Phone: 586041483
Administrative Phone Extension: ---
Administrative Fax: 8657586041483
Administrative Fax Extension: ---

Most recent unredacted registrant and administrative contact information of xclyd[.]com dated April 4, 2018.

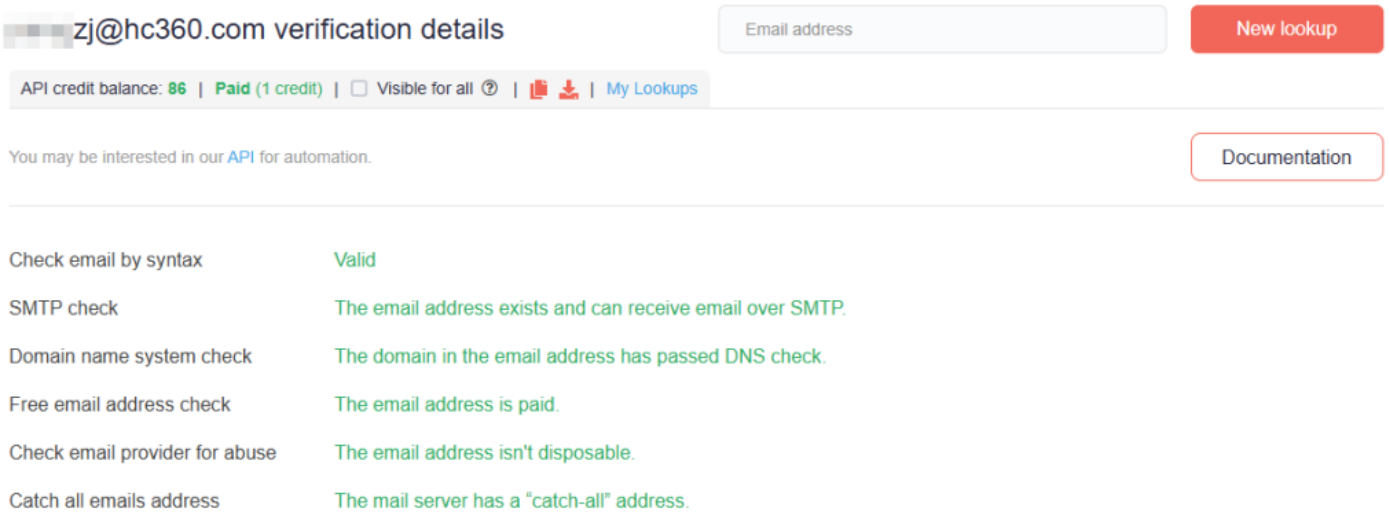
6. **Pivot**. Use that email or name to find other domains owned by the same actor. A historical reverse WHOIS lookup for the latest unredacted email address (****7337@qq.com) led to five other domains registered using that email address.



On the other hand, the oldest email address associated with the domain yielded 3,168 connected domains.

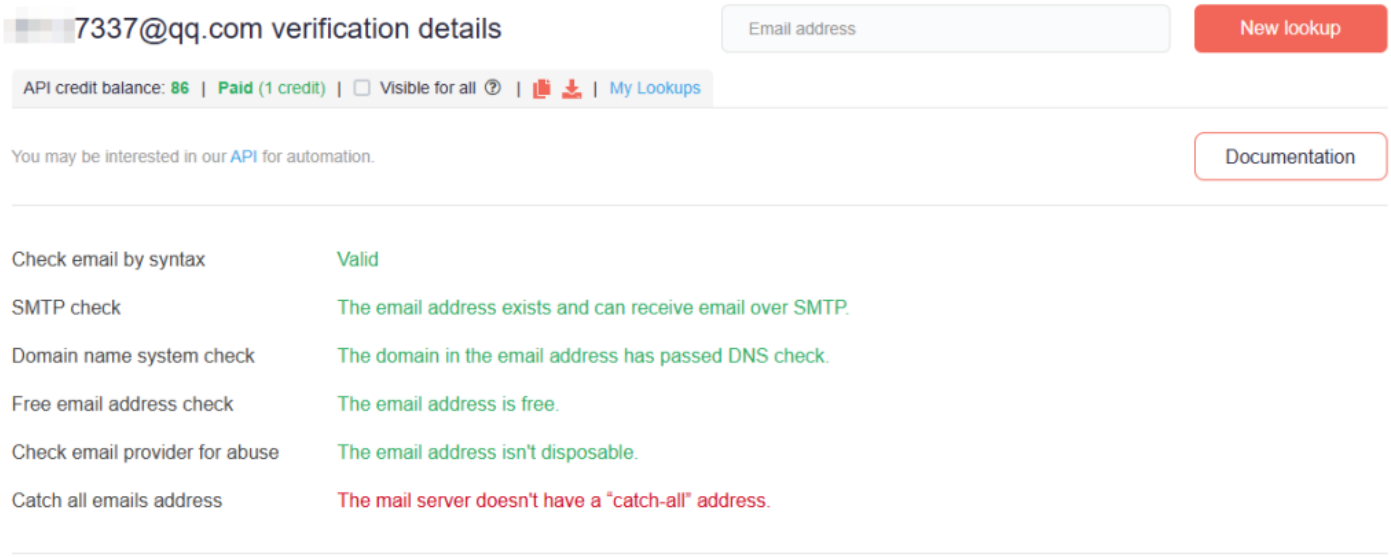


7. **Check email validity**. Now that you have two email addresses, you can try to see if they are still active. A quick check on Email Verification Lookup tells us that the email address can still receive messages.



Email verification results for the oldest administrative email address of xclyd[.]com.

The same is true for the registrant email address from 2018.



This is how you can retrieve domain WHOIS data after redaction. WhoisXML API's WHOIS History data is also available in the form of a lookup tool, database download, and an API.

If you wanted to replicate the same example as above with the WHOIS History API using a curl command and write the output into a JSON file, the query would look like this:

```
curl "https://whois-history.whoisxmlapi.com/api/v1?apiKey=YOUR_API_KEY&domainName=google.co
```

In the above example, you'll need to replace YOUR_API_KEY with your actual API key that you can get upon signing up.

Use Domain Info API

Domain Info API is a lighter alternative to a full WHOIS history search. While WHOIS History gives you a timeline of every change, Domain Info provides a single record that summarizes the most

relevant data for a domain.

It is more affordable and can be accessed via API, a lookup tool, or as a part of DRS. It helps you see data that was lost to redaction (if there ever was any), but it doesn't bypass paid WHOIS privacy services. If a domain owner had been using a privacy proxy, the tool will still show the proxy details.



Domain Info Search result for xclyd[.]com.

Domain Info is usually the easier alternative to WHOIS history when you need to use it in automated workflows, as you only get one WHOIS record instead of dozens.

An example API request to get the same result as above looks like this:

curl “https://domain-info.whoisxmlapi.com/api/v1?apiKey=YOUR_API_KEY&domainName=xclyd.com”

Again, you’ll need to replace YOUR_API_KEY with your actual API key, which is the same for Domain Info API and WHOIS History API. The output is a JSON that looks like this:


```
{
  "domainName": "xclyd.com",
  "data": [
    {
      "fieldName": "createdDateISO8601",
      "fieldValue": "2015-05-14T02:01:42+00:00",
      "auditDate": "2026-03-19T05:59:06+00:00",
      "isEmptyOrRedactedNow": false
    },
    {
      "fieldName": "updatedDateISO8601",
      "fieldValue": "2026-03-15T13:32:34+00:00",
      "auditDate": "2026-03-19T05:59:06+00:00",
      "isEmptyOrRedactedNow": false
    },
    {
      "fieldName": "expiresDateISO8601",
      "fieldValue": "2026-05-14T02:01:42+00:00",
      "auditDate": "2026-03-19T05:59:06+00:00",
      "isEmptyOrRedactedNow": false
    },
    {
      "fieldName": "createdDateRaw",
      "fieldValue": "2015-05-14 02:01:42 UTC",
      "auditDate": "2026-03-19T05:59:06+00:00",
      "isEmptyOrRedactedNow": false
```

```
},
{
  "fieldName": "updatedDateRaw",
  "fieldValue": "2026-03-15 13:32:34 UTC",
  "auditDate": "2026-03-19T05:59:06+00:00",
  "isEmptyOrRedactedNow": false
},
{
  "fieldName": "expiresDateRaw",
  "fieldValue": "2026-05-14 02:01:42 UTC",
  "auditDate": "2026-03-19T05:59:06+00:00",
  "isEmptyOrRedactedNow": false
},
{
  "fieldName": "nameServers",
  "fieldValue": [
    "NAOMI.NS.CLOUDFLARE.COM",
    "VASILII.NS.CLOUDFLARE.COM"
  ],
  "auditDate": "2026-03-19T05:59:06+00:00",
  "isEmptyOrRedactedNow": false
},
{
  "fieldName": "whoisServer",
  "fieldValue": "whois.gname.com",
  "auditDate": "2026-03-19T05:59:06+00:00",
  "isEmptyOrRedactedNow": false
},
{
  "fieldName": "registrarName",
  "fieldValue": "Gname.com Pte. Ltd.",
  "auditDate": "2026-03-19T05:59:06+00:00",
```

```
      "isEmptyOrRedactedNow": false
    },
    {
      "fieldName": "status",
      "fieldValue": [
        "clientTransferProhibited"
      ],
      "auditDate": "2026-03-19T05:59:06+00:00",
      "isEmptyOrRedactedNow": false
    }
  ],
  "registrantContact": [
    {
      "fieldName": "name",
      "fieldValue": "Registry Registrant ID: Not Available From Registry",
      "auditDate": "2022-04-29T07:16:11+00:00",
      "isEmptyOrRedactedNow": true
    },
    {
      "fieldName": "organization",
      "fieldValue": "Zhe Jiang Li Yong Da Zhi Ling Ji Xie You Xian Gong Si",
      "auditDate": "2018-04-04T16:49:33+00:00",
      "isEmptyOrRedactedNow": true
    },
    {
      "fieldName": "street",
      "fieldValue": "Xin Chang Cheng Dong Xin Qu Yu Lin Lu 18Hao",
      "auditDate": "2018-04-04T16:49:33+00:00",
      "isEmptyOrRedactedNow": true
    },
    {
      "fieldName": "city",
```

```
  "fieldValue": "Shao Xing Shi",
  "auditDate": "2018-07-24T00:00:00+00:00",
  "isEmptyOrRedactedNow": true
},
{
  "fieldName": "state",
  "fieldValue": "HUBEI",
  "auditDate": "2024-12-26T01:49:11+00:00",
  "isEmptyOrRedactedNow": true
},
{
  "fieldName": "postalCode",
  "fieldValue": "...500",
  "auditDate": "2018-04-04T16:49:33+00:00",
  "isEmptyOrRedactedNow": true
},
{
  "fieldName": "country",
  "fieldValue": "UNITED STATES",
  "auditDate": "2026-03-19T05:59:06+00:00",
  "isEmptyOrRedactedNow": false
},
{
  "fieldName": "email",
  "fieldValue": ".....337@qq.com",
  "auditDate": "2018-04-04T16:49:33+00:00",
  "isEmptyOrRedactedNow": true
},
{
  "fieldName": "telephone",
  "fieldValue": "......6041483",
  "auditDate": "2018-04-04T16:49:33+00:00",
```

```
      "isEmptyOrRedactedNow": true
    },
    {
      "fieldName": "telephoneExt",
      "fieldValue": null,
      "auditDate": null,
      "isEmptyOrRedactedNow": true
    },
    {
      "fieldName": "fax",
      "fieldValue": "......041483",
      "auditDate": "2018-04-04T16:49:33+00:00",
      "isEmptyOrRedactedNow": true
    },
    {
      "fieldName": "faxExt",
      "fieldValue": null,
      "auditDate": null,
      "isEmptyOrRedactedNow": true
    }
  ]
}
```


We've edited some parts of the output in this article for privacy reasons, but if you run a WHOIS history lookup (whether via DRS or API), the data will be there.

Conclusion

WHOIS redaction has made the internet more private for users, but it has also made it safer for criminals to hide — and harder for cybersecurity researchers to investigate.

When you hit a wall with a redacted record while investigating a suspicious domain, your first option is to use WHOIS history to find old, unmasked data. If that fails, reach out to the registrar's abuse contact or consider legal options such as a subpoena.

Sign up for WHOIS History or Domain Info to retrieve historical WHOIS records for the domains even after the mass redaction.

