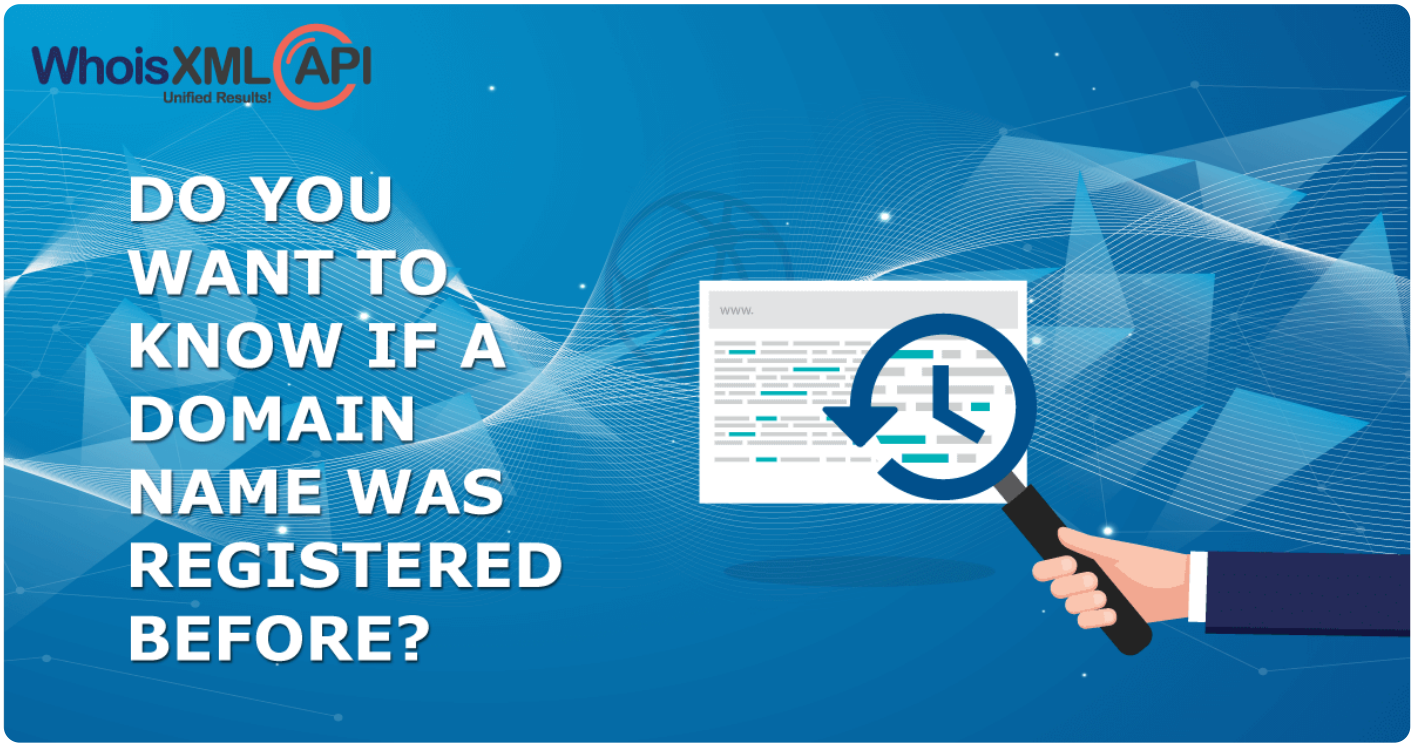
Research Any Domain’s History With Whois History API!

Posted on August 19, 2019



With thousands of new domain names registered every day, billions and billions have been registered over the years. And these have undergone multiple ownerships or even registration changes over time. These could be modifications to the domain's registrar or associated name servers or even changes in contact details, to name just a few.

Aging domains have a history and we at WhoisXML API can help you delve deeper to understand a given domain's past with WHOIS History API. Professionals conducting research for cybersecurity or investment purposes can hugely benefit from uncovering a domain's lifecycle to find out if it has ever had a checkered past or draw connections that may not be easy to see at the surface level.

Table of Contents

Why a Domain's Past Matters

We all know that if we're interested in purchasing a domain name for our company website, the easiest way to do so is by approaching a domain registrar. So we go online and look for domain

registrar recommendations and find the most popular ones. And that's hardly surprising, as any business would want to be served by the best. So we contact them and get a list of available domain names that would best fit our business requirements. We sift through the list and settle on one from, say, the top domain registrar according to our online research. Weeks after, perhaps, we launch our website and visitors start pouring in. Business is going well, that is, until we receive customer inquiries on our site's involvement in a cyber attack.

Are we being hacked? Has our website recently been owned so we've been directing visitors to phishing sites? We dig deeper. And after several conversations with the complaint filers, we realize they dug something up from our domain's past. As it turns out, our company isn't to blame, our domain's shady past is. We should have known better to have found everything we could on our domain's history before actually buying it. Too late for that though so we do the next best

thing—we issue a statement on our website severing us from ties to any malicious activities and assure our visitors that our pages are safe to visit.

If you don't want to be in this kind of situation, you'll need to be more careful when acquiring domains. One way to do that is by using a **WHOIS history API**, search, or lookup tool that will give you all the information you need on a domain. And we're not talking about just its current state but its past (no matter how clean or sordid it is) as well.

Looking into a domain name's entire history is critical if you don't want to be hounded by skeletons in its closet once your business is already up and running. Here are just some of the possible reasons why:

- **SERP violations:** In general, old domains are more likely to get better SEO rankings because they have been online for quite some time. But that's only good if they were ranked for a good reason. Typical examples of this would be great content, tons of visitors, and so on. But some aged domains may have been abandoned by their former owners because they had been flagged for violations. That said, no matter how good your SEO strategy is, your pages will never get good rankings because they've been marked for bad behavior. Be sure not to end up with such a domain or you'll suffer the consequences of its previous owner's wrongdoings.

- **Ties to cybercrime and cyber attacks:** The domain could have been involved in a past crime. Cybersecurity solutions block access to identified malicious URLs from their customers' systems. If that's the case, potential clients who wish to visit your website would always be alerted to its insecurity (based on historical data) through warnings. They'll never reach your site and that means lost opportunities for your company. Compromised URLs that end up as unknowing accomplices to cybercrime also get named in threat reports and news. That's most likely how the site visitor in our sample scenario ended up complaining about our site's safety.

- **Hijacked domains:** Not all domains that end up seemingly "available for use" have been lawfully obtained. Some could have been stolen from other individuals or organizations. And the only way you can use them is because they have been compromised by the ones selling them. This is easy to do with insufficiently protected domains. Make sure you don't end up

buying a stolen domain or you just may lose more than you gained.

- **Ties to unscrupulous content and activities:** Some websites may have been taken offline by the authorities because they contain malicious content (porn, etc.), sell fake goods and services, or have ties to illegal activities. Make sure the domain you're currently eyeing didn't play host to such sites or you'll land in hot water.

- **Handing your personal data and money to fake registrars:** Not all registrars that advertise on the Web, especially those who offer really low prices, are legitimate. If you've got your heart set on a domain and finally found just one registrar that offers it, conduct extensive background research on the seller first. More often than not, the most promising domain names are already taken and just because you found someone offering your dream domain doesn't mean you've hit the jackpot. Be very wary about hard-to-believe offers, as they almost always end up being false. You may just be taken in by a fake domain registrar.

Domain registrars often buy domains in bulk for reselling. They may not have had time to check all of their purchases' past (or may just not care). It doesn't help that even the best and most reputable registrars have also had brushes with the law. Take a closer look at these noteworthy incidents:

- **Alibaba Cloud Computing:** Several domain names tied to an Android supply chain attack just this June were reportedly registered by this provider. The attack perpetrators used these domains to preinfect Android-based smartphones with malware before they even came off the rack and made their way into mobile phone shops.

- **Google Cloud Platform:** Thousands of vulnerable D-Link routers were affected by a spate of traffic redirection attacks. Hackers abused the provider's network to reroute the traffic that passed through affected routers to malicious sites, putting the victims' systems and the data they contain at great risk just this April.

- **Namecheap:** Sometimes, the more popular a registrar is, the more likely cyber attackers will go after it. That's because halting its operations means affecting a greater number of websites. This is a lesson that providers such as Namecheap and other big names like it learn the hard way.

But since you're the one whose brand and therefore reputation is at stake, you want to make sure you won't regret using the domain name you chose.

Dig deep into the past of your business's gateway—your domain—so its ghosts won't end up haunting you with WHOIS History API.

What WHOIS History API Reveals

Every company website has its own WHOIS record. It's required by law. And any site owner who provides false information on this record is penalized (his ownership is rendered null and void). That said, all registered sites' WHOIS records are stored in a database that anyone can access through API, search, or lookup tools. There are tons available on the Web today though not all of them let you do **historic WHOIS lookups** — the kind you need to do to find out everything about a domain name's past.

Apart from providing typical information found in a WHOIS record — registrant and billing, administrative, and technical contact name and details; registrar; nameservers; registration and expiration dates; and so on — you need a **WHOIS history search** tool that will give you data on how many changes (registrant, contact details, nameservers, etc.) a domain has undergone throughout its existence and when these occurred. That way, you can find out if it has been involved in any kind of activity that can be harmful to your business. If our sample scenario has taught us anything, that means don't purchase that domain name.

When looking into a WHOIS record, don't stop at finding out all you can about its content. Look for signs of malicious ties as well to its registrar, registrant, contacts, nameservers, and everything else on its historical records.

But what makes a great **WHOIS history API**, search, or lookup tool? Find out in the next section.

What You Should Look For In A WHOIS History Database

A **WHOIS history API** is only as good as its source — the WHOIS history database it's hooked to. A good database is one that contains billions of WHOIS records that span the entire TLD space. It

not only has records on domains that use popular gTLDs such as .com, .net, and .org, but also the more uncommonly seen ccTLDs like .tk, .ru, and .cn, along with those that sport newly created gTLDs such as .xyz, .biz, and .shop. Look for the complete list of TLDs that it supports so you can check if it's as comprehensive as it says on its website. Choose a provider that has been in the business for a good long while. That's one way to find out how reliable its product is. It also gives you an idea of how far back its domain historical data goes. Is it recommended by reputable companies? That will help you make sure that it's not just tooting its own horn. Find out what its clients actually say about the tool.

WHOIS History API gives you access to:

- More than 5.2 billion WHOIS records
- More than 582 million domains
- More than 2,864 TLDs
- More than 10 years' worth of WHOIS data

Because the tool contains a consistent set of WHOIS information, it can be easily filtered based on date (registration, expiration, and modification) for easy analysis.

WhoisXML API has been in the business for almost a decade with product recommendations from more than 50,000 of today's biggest online brands such as Apple, Amazon, GoDaddy, and more. Backed by a solid foundation, **WHOIS History API** can give you timely, accurate, and relevant information on any domain throughout its life cycle to meet several business needs—cybersecurity, brand protection, fraud investigation, and many more.

To get a glimpse of the many benefits that a **WHOIS History API** provides, see the list we compiled in the next section.

What You Can Do With Historical WHOIS Data

Historical WHOIS data can be useful for many kinds of business applications in various industries. Here's a list of who can benefit from using **WHOIS History API** and how:

Potential User	Practical Uses
Cybersecurity professional	Gather currently hidden information on a privately registered website by looking at its history
Domain registrar	Sift through registrant changes to make sure the domain you're looking to buy doesn't have anything to hide

Potential User	Practical Uses
Fraud investigator	Find out how long a case has been occurring by going back in timeto look at a domain's entire life cycle
Marketing professional	Get to know your customers better to keep them coming back for more

With **WHOIS History API**, you get a whole lot more information than you would normally find in a regular WHOIS record. To ensure your business's future success, it's not enough to focus on what's right before your eyes, it's also critical to carefully assess the past so you can avoid bad surprises when you least expect them.

WHOIS History API results can be downloaded in two easy-to-read-and-decipher formats —JSON (readable on any text editor such as Notepad on Windows and TextEdit on Mac OS) and XML (readable on any spreadsheet application like Microsoft Excel on Windows and Numbers on Mac OS). You don't need to purchase additional software to use it. To see sample WHOIS History Reports and nifty tips and tricks on using it, visit this page.

WHOIS History API is just one of the many tools in WhoisXML API's Enterprise API Package. To get the most out of domain monitoring, use it with these other tools:

- **Enterprise Data Feed Package:** This works best for users who prefer sifting through and analyzing data offline. It comes with:
  - **WHOIS Database Download:** This provides partial or complete historic domain information that can be customized according to your business needs.
  - **IP Geolocation Data Feed:** This is an exhaustive and precise IP geolocation database that is updated on a weekly basis.
  - **IP Netblocks WHOIS Database:** This lets you find out which IP range a particular address belongs to, along with its owner's contact and other information.
  - **Domain IP Database:** This gives you access to the biggest passive DNS database

that works particularly well when you're conducting cybersecurity research.

- **Enterprise Tools Package:** This, meanwhile, works best for those who prefer working with data online. It comes with:
  - **Domain Research Suite:** This enhances your domain research toolkit with enterprise-grade Web-based solutions that help you search for and monitor domain-related data. It comprises:
    - **Reverse WHOIS Search:** This lets you find all domains containing specified search terms in their WHOIS records.
    - **WHOIS History Search:** This is **WHOIS History API's** Web-based counterpart for those who want to find all there is to know about a domain's past on a Web interface.
    - **WHOIS Search:** This allows you to get all the key data points related to a domain name you're interested in.
    - **Domain Availability Check:** This lets you find out if the domain name you want to purchase is available for registration.
  - **Whoisology:** This is an advanced reverse WHOIS tool that lets you find deep connections between domain names and their owners. It was primarily designed for cybercrime investigations, intelligence gathering for infosec and corporate use, conducting legal research, and business development.
  - **Threat Intelligence Platform or TIP:** This is a set of enterprise-grade threat intelligence tools for optimal threat detection and analysis. It makes use of the following APIs:
    - **Domain's Infrastructure Analysis API:** This lets you research servers'

infrastructure beyond their domain names.

- **SSL Certificates Chain API:** This obtains a domain's SSL certificate, along with its certificates chain in a well-parsed JSON format.
- **SSL Configuration Analysis API:** This allows you to check a host's SSL connection and analyze it for common configuration issues.
- **Domain Malware Check API:** This lets you check if a domain name has ties to malware.
- **Connected Domains API:** This lets you discover domain names that resolve to the same IP address.
- **Domain Reputation Scoring API:** This allows you to evaluate a domain's reputation based on several security data sources using an instant external configuration auditing procedure.

Whether used as a standalone tool or in combination with other domain monitoring and research tools, **WHOIS History API** is sure to give you all the information you would need to make sure your domain is as threat-free as it can possibly be, thus ensuring not just your company's safety, but also that of your employees, clients, partners, and other stakeholders.

WHOIS History API will not only give you useful insights into the entire history of the domain you're interested in purchasing, it can also help you beef up your company's security posture by blocking sites with known ties to malicious actors and activities; get to know your customers, partners, third-party suppliers, and other stakeholders better so you can enhance the way they do business with you; spot domains with potential tie-ups to outstanding fraud cases; and so much more. How? The next section will tell you.

How WHOIS History API Works

Immediately after registering for the service, you can start reaping the benefits of **WHOIS History API**. Here's how:

- 1. Log in and type the name of the domain you wish to see the history of into the search field.
- 2. You will see how many historical records the domain has had over the years beside "Historical records discovered" and how much the reports would cost if downloaded in either XML or JSON format next to "Report price."
- 3. Below these, you can see a preview of the reports you can download. You can filter information by update date, registrar name, WHOIS server, and other WHOIS data.

Now you're all set, you can dig as deep as you want on any domain's past. The next question you need to answer is "What specific threats should you be looking for to make sure your domain's past won't haunt you?" The next section gives you an idea.

Specific Threats in Your Domain's Past That Can Harm Your Business

Although the World Wide Web allows users to transcend boundaries set by time and space, it is also chock-full of threats that any business wouldn't want to be caught having ties with. With **WHOIS History API**, you can look out for these to make sure your domain's past won't cause you grief:

- **Phishing:** Cyber thieves sometimes hijack insufficiently protected websites to redirect users to their own specially crafted data-stealing pages laced with keyloggers to siphon log-in credentials.
- **Spamming:** Threat actors normally spoof popular companies to send out spam that either come with malicious attachments that, when opened, infect users' computers with malware (typically data stealers) or links that point to websites that drop malware onto users' systems.

- **DDoS attack:** One way by which cyber attackers hide traces is by using compromised sites to do their malicious bidding. In DDoS attacks, for instance, they transform vulnerable sites into bots that disrupt the operation of their targets.

- **Cryptocurrency-mining malware:** Cybercriminals typically plant these into company websites so they don't use up their own resources to generate cryptocurrencies that they can use to fund their operations or sell for profit.

- **Business email compromise or BEC:** Also known as email account compromise or EAC, fraudsters typically pretend to be C-level executives of organizations to trick employees who have access to financial resources into transferring huge sums of money into the attack perpetrators' accounts.

- **Malvertising:** Cybercriminals typically plant malicious advertisements in unsecured sites so they won't need to create their own websites or pages just to get to victims. They just need to bait compromised sites' visitors into clicking their ads.

This list is by no means exhaustive. Any ties to an online attack, even if it happened years ago can land your business in hot water. Remember that security companies and authorities can block access to your domain, IP address, or website when these are used in any kind of cyber attack. So even if you're an innocent victim or unknowing accomplice, your company may suffer dire consequences. This is exactly why you need to ensure your domain's safety at all times and why it's important to know everything about it before you even start using it. Your domain's past can make or break your business's current and even future state.

Concluding Thoughts

Your domain is your business's online home. It's the place where employees feel safest. And so you should make sure it will not get hacked, thus not putting your staff at risk. It's also where you welcome guests so make sure it won't serve as host to malware or redirect them to malicioussites. That's why you must always make sure it stays protected against all kinds of online theft.And to some, it's also where they work and so it must remain secure from anyone who wishes itany harm.

Don't let your name suffer just because you happened to choose a domain name with a shady past. Remember that a name is only as good as its history. What good would a great domain name do if it comes with a lot of unwanted baggage? Use **WHOIS History API** so you won't need to clean up your act even before you make a mistake. Living with your past mistakes is hard enough, so why live with someone else's?

More Information on WHOIS History API

For those interested in putting WHOIS History API to work, note that it is part of our Domain Research Suite. As such, API requests are charged in so-called "DRS credits." This is a convenient way to use all of the products in the suite with a single subscription that works for both the APIs and Web-based search tools. Costs vary according to the operation you require. One **WHOIS History API** request costs 50 DRS credits.

Signing up is free of charge and gives you instant access to the API. We also offer one-time purchases to those who don't have a recurring need for domain information. Monthly and annual subscriptions packages, meanwhile, should serve those who regularly use domain data better. For more detailed pricing information, see the pricing table on this page.

If you're looking for more customized plans, feel free to contact WhoisXML API at sales@whoisxmlapi.com. What are you waiting for? Find out all you can about any domain's past with WHOIS History API.