WHOIS History Lookup: 6 Illustrative Use Cases

Posted on September 27, 2018

Today's lesson is about history.

Specifically, about WHOIS History Lookup and WHOIS History API.

Both are tools for tracking historical WHOIS records of domain names to find out how their ownership has changed over time. We've been doing it for more than 10 years and have compiled more than 300 million active domain names, 1 billion history domain names, and 5 billion historical WHOIS records in our database.

Everything is available to our users.

Relevant historical WHOIS records include the dates when the target domain was created, updated, or when it expired; the registrant's name, address, and contact information; as well as the name of the registrar. Also included are the array of name servers; the WHOIS server and raw WHOIS record; and the administrative, technical, billing, and zone contact information.

Why are they so important?

Because if we are not aware, something unpleasant that has happened in the past is bound to be repeated.

WHOIS History Lookup and **WHOIS History API** can keep you informed and alerted on the threats of cyber attacks by looking deep into the past and using the insights to guide your steps when moving forward.

Here are six ways in which historic WHOIS data becomes an invaluable tool to safely navigate the digital domain space.

1. Ensure Efficient Marketing

These days, establishing a web presence plays a crucial role in marketing. That requires having a domain name that's unique and could figure prominently in SEO rankings. With hundreds of millions of domain names all competing for attention, however, making the right choice could be tough if you don't know where to look.

WHOIS History Lookup helps by finding out if the domain name that you have in mind is still

available. If it's been registered before, every aspect of its past will be scrutinized for any history of malicious activity.

The result will help you decide on the right domain purchase, guide you on your planned product launches, and enable you to take defensive measures if necessary. A careless domain choice could end in bad publicity that would affect your image and negate your marketing efforts.

2. Safeguard Domain Reputation

Good reputation is the foundation of a successful business. That's the reason why companies that have been involved in shenanigans have their names crossed out from public lists.

WHOIS History Lookup and **WHOIS History API** help safeguard your good name by finding out if the website has been engaged in shady activities or shares a hosting server or IP address with malicious domains.

This prevents you from being mistakenly associated with cybercriminals, which in turn could get you excluded from search engine results or have your email delivery blocked.

Other ways **WHOIS History Lookup** steers you away from trouble is by finding out if the website was stolen, if its previous version distributed sensitive content, or if it was owned by questionable characters.

3. Review Third-Party Credibility

Collaborating with third-party suppliers could turn out to be a pact with the devil if you're not careful. They could be hatching evil plans, or cyber criminals could be using them to get to you.

Reviewing historical WHOIS records will help you assess the credibility of third parties. **WHOIS History API** will tell you where and when they were registered. You will be alerted once they are found to have been connected with malicious domains, or if their owners have had bad records. Any detail that raises a red flag should give you sufficient warning to keep your distance.

4. Assist During Investigations

WHOIS History API helps law enforcement authorities fight cybercrime by providing leads and turning up evidence of fraudulent intent.

Those include:

- Tracing the history of suspicious domains and their connections with other malicious entities on the Web;
- Gathering leads on the authors of malware and the websites that are spreading them;
- Analyzing patterns of fraud to uncover new variations of cyber threats from hackers;
- Finding information that identifies persons of interest who can be contacted for questioning.

5. Enforce Cybersecurity

Insights gained from analyzing historical WHOIS records provide invaluable inputs in improving cybersecurity efforts.

For one, cybersecurity specialists can examine the origins and techniques of hackers once they have identified the malicious websites that had posed threats or attacked companies. Once their history has been established, cyber specialists can use the findings to block malevolent IP addresses, update firewalls, or block malicious websites at the network firewall layer.

6. Help Registrars & Domainers

Historical WHOIS data are a big help to registrars and domainers who can use the information on the ownership and other specifics of certain websites to fully address questions from their new owners. Other than that, learning the history of malicious websites can alert them to possible issues that could emerge in the future. Registrars, particularly, will be sufficiently informed to provide reliable and secure domain name ownership transfer and management to registrants. Domainers, on the other hand, will be able to check for availability of domain names as they occur.

Learning about the history of a domain using **WHOIS History Lookup** has many practical applications. It strengthens cybersecurity, enhances marketing efficiency, fights cybercrime, and ensures the credibility of third parties. Best of all, it safeguards a domain's reputation which is the foundation of business credibility on the Web. For more information, check out WHOIS History Lookup and WHOIS History API or contact us at general@whoisxmlapi.com.