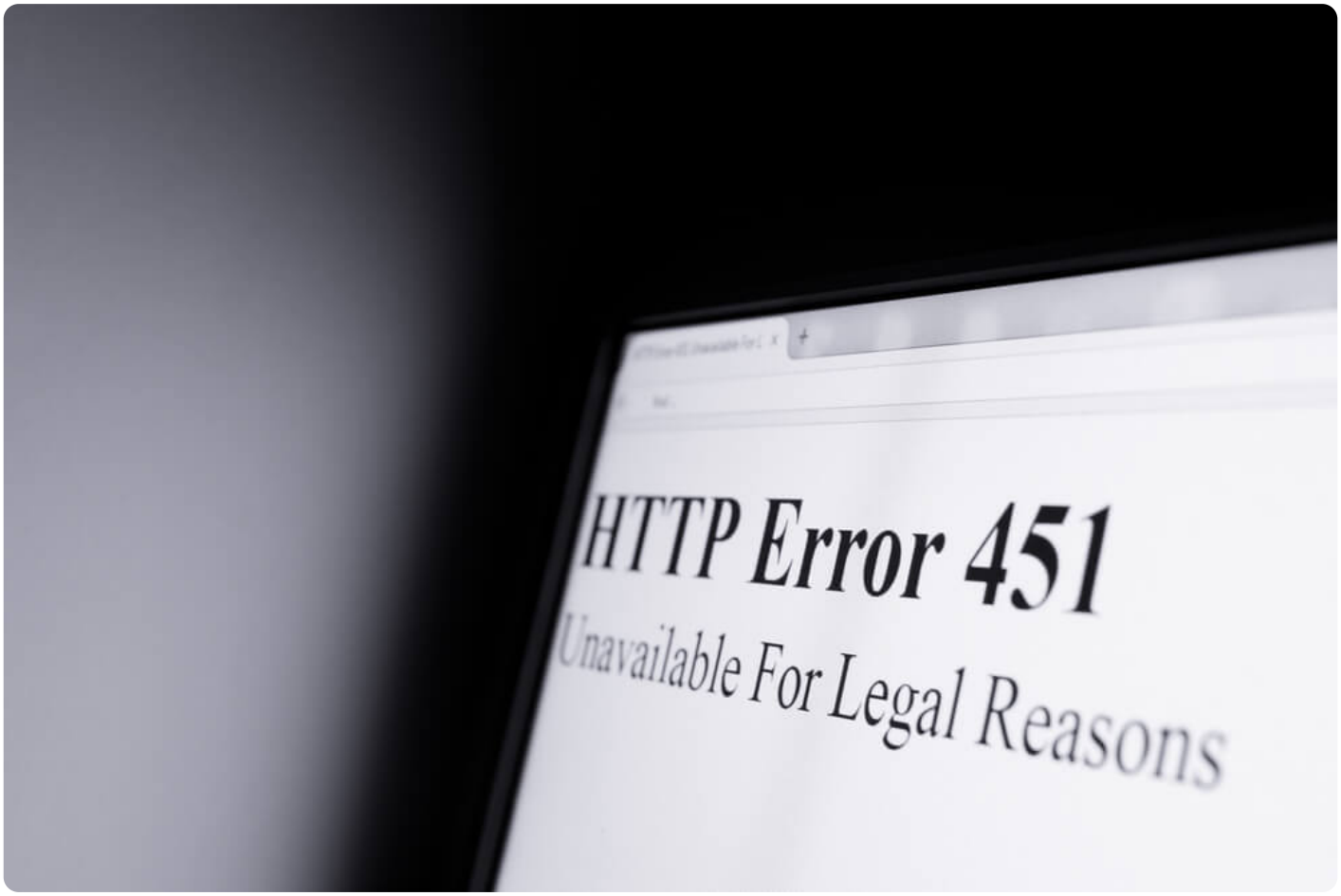
How Organizations Can Prevent Site Blacklisting with WHOIS History Search and WHOIS History API

Posted on March 5, 2020



Maintaining the overall health of your site is no mean feat. Attacks could occur any time, regardless of a company's size. Cyberattackers can hack into your network and compromise your site for use in their nefarious activities without your knowledge. Sometimes, you'll only know what happened when search engines like Google put your site on a blacklist. And that can be detrimental to any business. Blacklisted sites may lose around 95% of their usual amount of organic traffic, which can negatively affect their sales. Apart from that, first-time visitors or potential customers can get discouraged if they learn that your site is considered malicious.

Table of Contents

Race Against Time: Getting a Site Off a Blacklist

When your site is blacklisted, your web administrator needs to race against time to rid it of malicious content or malware and then get back to Google, so it can be recategorized as safe for users to visit once again. Web administrators and site owners are encouraged to use proactive security solutions and put countermeasures in place so they don't have to go through the hassle of cleaning their site while conducting a root cause analysis (RCA) and losing their customers' trust in the process.

To prevent your site from becoming part of a blacklist, you first need to know what may cause it to be blocked. Here are some of the reasons why search engines blacklist sites:

- **Malware presence:** Cybercriminals use compromised sites as malware distributors in drive-by download attacks. The most dangerous malware types hosted on breached sites probably include ransomware and information stealers. Unsuspecting visitors typically don't even have a clue when their computers get infected.

- **Spamming:** Some compromised sites are embedded with links to known spammy pages. In some cases, blacklisted sites unknowingly feature malvertisements. And because any ties to malicious activity, no matter how trivial, negatively affect all the connected sites' reputation, these may end up blacklisted as well.

- **Phishing:** Some attackers inject malicious codes or scripts into breached sites to redirect visitors to phishing sites designed to steal their login credentials and other personally identifiable information (PII).

- **Inappropriate content:** Adult and harmful or offensive content hosted on sites can also make them part of a blacklist.

Cyber attackers often prefer to compromise legitimate sites instead of creating fake ones so they can abuse the established trust between the affected businesses and their customers. This approach guarantees that their attack will affect as many people as possible.

Bearing the above in mind, this post looks at the case of several websites that Google may consider for blacklisting and how tools such as WHOIS History Search and WHOIS History API can help avoid online properties that were found malicious in the past.

Hacking and Vulnerabilities: Where Blacklisting Can Start

Cyber attacks can break businesses, as these three cases show:

- OnlyHonest.com: The site was about to turn one year old when Anonymous, a well-known hacktivist group, hit it. OnlyHonest.com, which allowed users to debate with each other on political topics using videos, was making its mark with users, networks, and advertisers even on social media when it was defaced. Anonymous actors defaced its every page with digital graffiti. But every time the owners removed it, the attacks escalated. At one point, the hackers even redirected all of the site's traffic to another site.

  This attack forced the owners to take down the website even if it already contained hundreds of user videos and had 10,000 Twitter followers. They struggled to secure funding to make the site safe again before they try to relaunch it. Years after, they didn't succeed, and the domain is now up for sale.

- CreditNerds.com: Customers alerted the owner that his website had been attacked. He received a considerable number of phone calls from people saying they were getting alerts when they tried to access the site. Later on, it was found that a piece of malware had infected CreditNerds.com, which helped consumers repair and improve their credit standing. The malicious code infected the site's every page. Although the clients' information, including dates of birth and Social Security numbers, wasn't compromised, the owner decided to take down and replace the site. He also changed hosting providers. He spent $3,500 rebuilding the site.

  Before the attack, the then five-year-old business got 10 to 15 new customers each week. This number dropped to zero in the 10 days that the attack ensued. The site owner estimated around $9,000 in lost revenue. To remedy the situation, he went without pay for several weeks, but his business survived somehow.

- MintGreenMarketing.com: The Federal Bureau of Investigation (FBI) once contacted the owner and informed her that her site was compromised. The company was already a decade-old business that provided marketing strategies to small businesses. The FBI said the website was infiltrated by threat actors that injected malicious codes into its file structure. Also, its owner did not know that security filters had been blocking access to her website. She was advised to rebuild her site from scratch, which cost a few thousand dollars. And

after that, some Internet service providers (ISPs) still blocked the URL for security reasons.

All of the violations the featured sites were tagged for could have them end up on a blacklist, causing their businesses to suffer.

What Site Owners Should Do to Avoid Blacklisting

Apart from the commonly known guidelines such as making sure your site is not serving as a launchpad for fraudulent activities, you can also follow the below checklist:

- Avoid copying content from other sites without their owners' permission. Some businesses that wish to get traffic to their sites copy others' content. Google flags them for fraud. Keep in mind that original and relevant content drives traffic to any site.

- Make sure your site content passes GoogleBot standards, regardless of the language used (i.e., for sites with regional versions) or device used to access it (i.e., web or mobile). Keep links to spammy pages off your sites.

- Never use blackhat search engine optimization (SEO) techniques just so your site gets a higher search engine results page (SERP) ranking. Cybercriminals are known for tampering with SEO results, so compromised or malicious sites turn up as top search results for unsuspecting users.

What To Do When Google Blacklists Your Site

Getting your site off Google's blocklists is a daunting and time-consuming task. It is also resource-intensive, especially for small businesses that may not have threat response teams.

The process may include, for instance, checking out which parts of the site are infected with malware then cleaning them. Resetting account passwords is also highly advisable to thwart attackers from further infiltrating your network and get access to exposed servers and databases.

Make sure as well that attackers did not create additional web administrator accounts. Doing so could help them do more sinister stuff on your network. Only when you're 100% sure your site is free from infection and any malicious modifications should you contact Google to reevaluate it. This process may last a few hours to several days.

Site blacklisting can have severe repercussions for your reputation and bottom line. It is highly advisable, therefore, to approach site safety with caution. Integrating tools such as WHOIS History API into your server or subjecting each connected site or page to a WHOIS history search can proactively protect your organization from the pain and hassle that site blacklisting can bring.

Potential Solutions: How WHOIS History API and WHOIS History Search Can Help

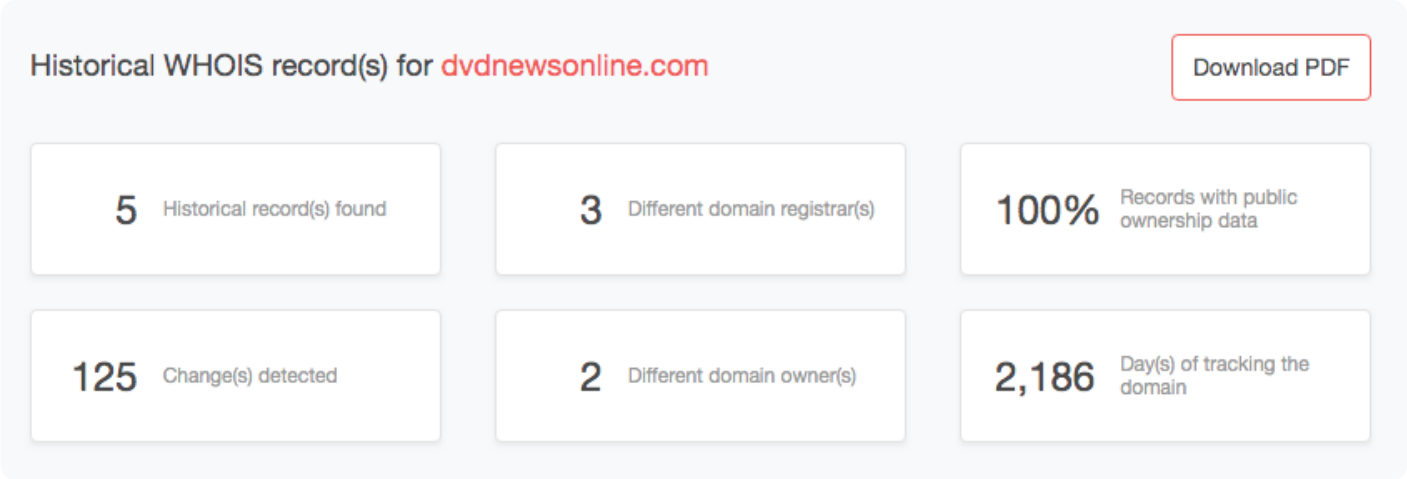
Domain research and monitoring tools such as WHOIS History API and WHOIS History Search can shed much-needed insight into a domain's past. They can be used to profile all of its previous owners, their organizations, and related activities. The tools can help bring potential issues to the fore, such as potential ties to cybercriminal groups, cyber attacks, illegal content (e.g., shocking sites, fake goods, etc.), and other unscrupulous activities. They are also particularly helpful to business owners who are looking for an old or expired domain (because it can attract more traffic) to purchase. In that last case, the tools can help them do thorough background checks.

Take a look at the following demonstration to see how the tools work:

- Let us say that a business owner is looking to purchase dvdnewsonline[.]com to host his business's website. (Note that we randomly chose the domain from the Stop Forum Spam database.) Ordinary users are not usually aware of such sources and so may end up purchasing untrustworthy sites. Type the domain name to see its history into the Search field.

- Our WHOIS history search results revealed that the site has five historical records. The WHOIS records on the tool appear from the most recent to the oldest (i.e., when the domain was first registered). Within its entire life cycle, it has had three registrars and two registrars,

and undergone modifications 125 times. The domain has been active for 2,186 days, or almost six years.



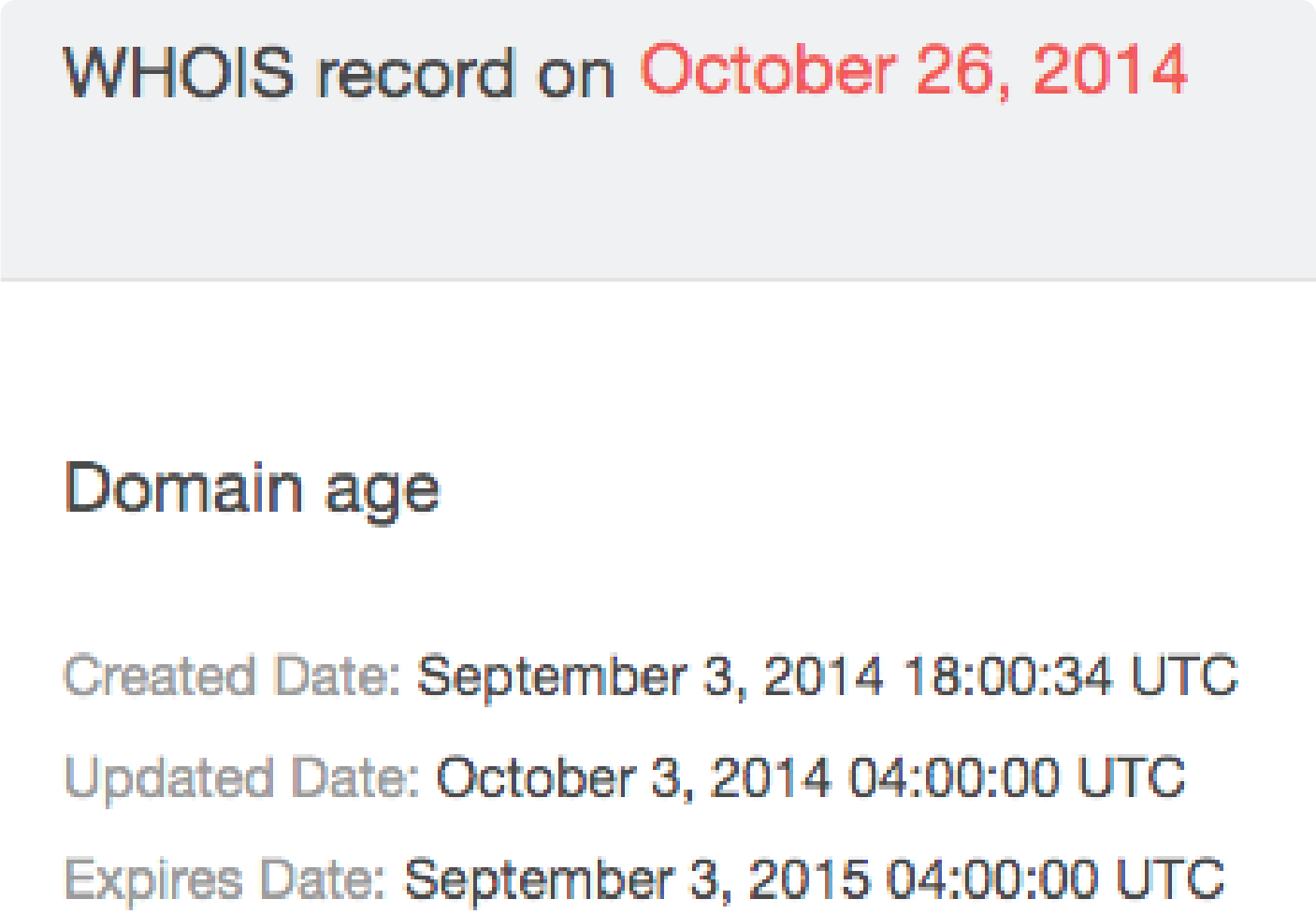
- Clicking a date from the list opens a corresponding WHOIS record. Each record reveals when the domain was created, last updated, and is scheduled to expire; who its registrar and registrant are; what its WHOIS and name servers are; its current status; and its contacts details. A thorough background should start by viewing the oldest record. In this case, it's the one dated back to December 4, 2013.

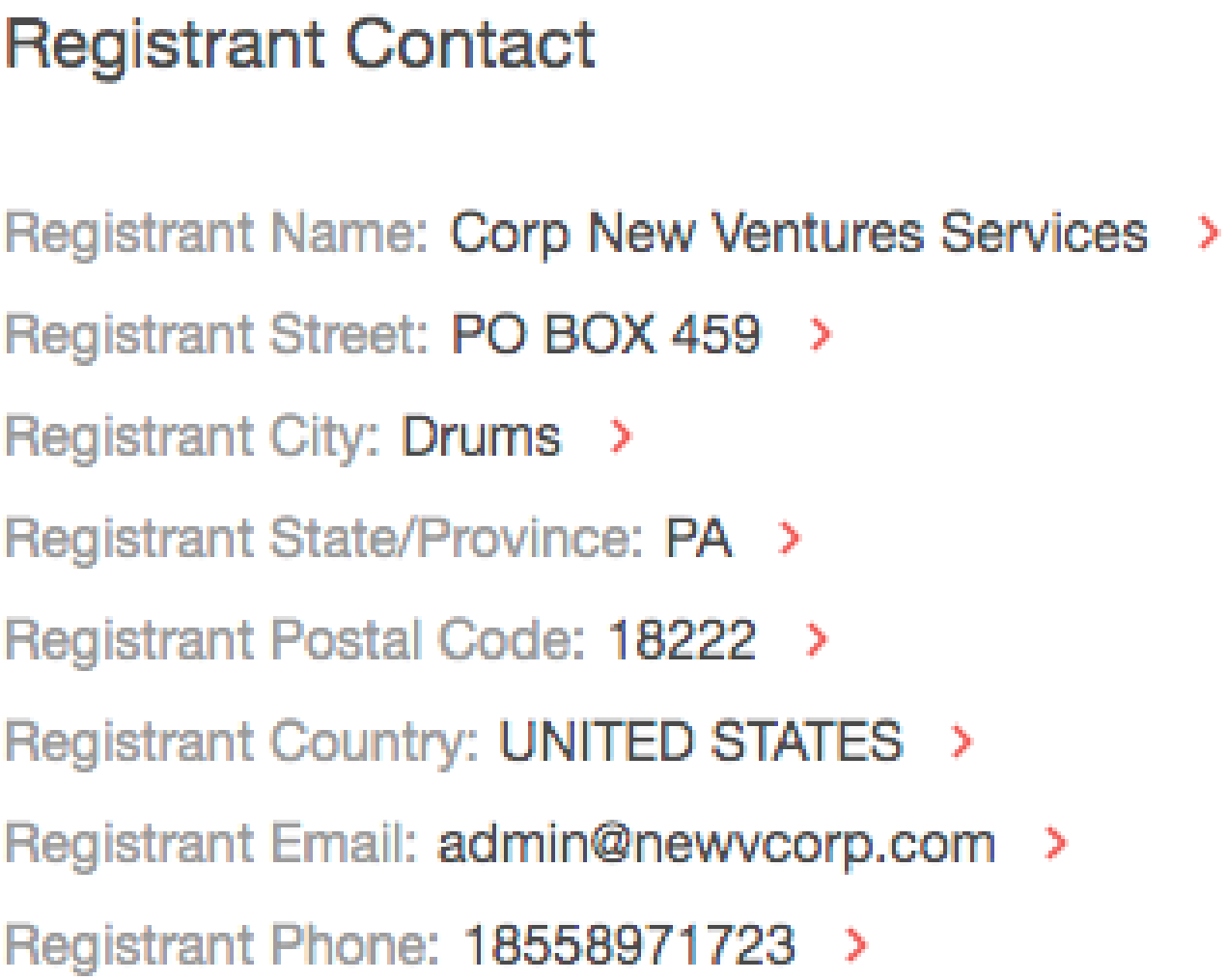
- We saw that the domain was created on June 25, 2013. If the business owner is looking for an aged domain, then it is a good candidate. Its registrar Guangdong JinWanBang Technology Investment Co. Ltd. is an established registrar, which is also good. An individual named Wu Youran from China registered it using the email address wujing.sm@gmail[.]com.

- Given all that, you can check each record and keep track of the same details, then search for the registrants' names, email addresses, and other domains for ties to malicious activities if any. To find out if a registrant owns other domains, you can use Reverse WHOIS Search. Just type the registrant's name or email address into the Search field and run the query.

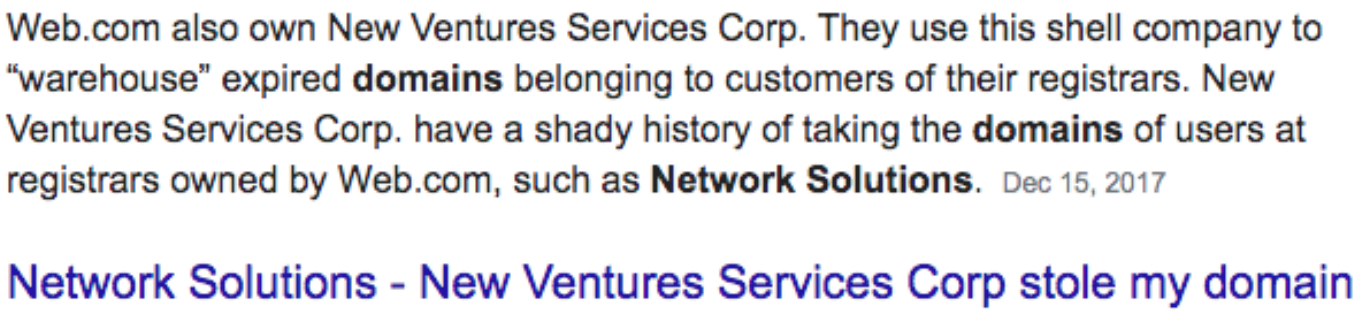
- Build a WHOIS report for each domain and check if any of them belong to the same registrant or used the same email address. Our particular query for the original owner did not return any other domain names.

- The domain, however, changed hands on 3 September 2014. Its new owner was Corp New Ventures Services.





- A quick web search for the registrant revealed this:



- All of the above indicates that the domain is probably not worth purchasing. If your web searches don't pan out or you want to ensure that you leave no stone unturned, you can search for more information from publicly accessible threat databases.

Historical WHOIS data is an excellent starting point for launching in-depth investigations on domains and their past owners. Apart from business owners searching for domains for their sites, such information can also benefit:

- **Cybersecurity professionals:** It lets them unearth details about domains involved in cyber attacks.
- **Domainers:** The data helps them screen the expired domains they may wish to purchase to make sure these don't have checkered pasts that may negatively affect their new owners if ever.
- **Fraud investigators:** It can reveal domains' and their owners' ties to fraudulent activities.
- **Marketing professionals:** The information helps them get to know potential customers better.

WHOIS History API provides the same information as the search tool. Unlike the web-based interface, however, it can be integrated into existing solutions and systems to allow them to automatically screen for all former registrants' potential reputation-tarnishing backgrounds.

Concluding with Best Practices and Recommendations

Search engines have strict rules and can sometimes be vague about their blacklisting policies. Google's inclusion policies, for instance, do not necessarily say what constitutes a violation that could land a site on its blocklist. So, Web administrators need to always be on guard and should continuously monitor their digital properties for threats.

The following are some best practices that they can adhere to:

- Update servers and software regularly. Applying patches can prevent attackers from exploiting vulnerabilities. We have seen exploit kits such as Angler compromise sites to redirect users to sites where its code is hosted.

- Keep an eye on your web server logs, especially access logs. Any web server appearing on the Internet is immediately subject to a tremendous number of attacks looking for possible exploits. Log files can reveal the resource the attackers were looking for, along with their IP addresses. On the one hand, this helps you make sure that the exploit does not make it into your system, or if it succeeded, you become at least aware of that and can take the necessary steps. On the other hand, the IP addresses of attackers can be sought for in an IP netblocks database to find out its owner. They can also be queried with an IP Geolocation API to localize your attacker.

- Regularly scan your site for malware or malicious scripts. It is better to be proactive rather than wait to get blacklisted before taking action.

- Check all third-party sites linked to yours. They may be blacklisted because of ties to spamming, phishing, and other nefarious activities. You can also use Threat Intelligence Platform for that purpose.

- Use web application firewalls to prevent hackers from inserting malicious codes or redirects

into your site’s pages.

- Use relevant and SEO-friendly content to generate more organic traffic to your website. Copying other sites’ content without permission may cause your site to be blocked by search engines.

Search engines want to keep their users safe from threats. That’s why they blacklist sites that do not meet their strict criteria or violate their policies knowingly or unknowingly. The consequences can be damaging. And so it is critical to keep your organization threat-free at all times with the help of tools such as WHOIS History API and WHOIS History Search.