How Can a Domain Reputation Lookup Tool Improve an Organization's Security Posture?

Posted on April 6, 2020

Many organizations only consider domain reputation in the context of email services and deliverability. They believe that scores only have to do with whether or not sites are seen as reputable email senders. However, that is not always the case. Domain reputation covers far more than that.

A good domain reputation score can be a stamp of confidence when it comes to website security. Therefore, it is imperative for organizations to regularly carry out **domain reputation lookups** with a tool like Domain Reputation API or Domain Reputation Lookup to assess both their own websites and those of external stakeholders to improve their security posture. Let's take a closer look at why it matters.

Poor Domain Reputation and Blacklisting: How They Affect Organizations

A poor domain reputation or affiliation with sites that have one could land your organization in a blacklist. And that can leave a bad taste among your clients and customers, which may ultimately affect your bottom line.

To avoid such a scenario, your security team must strive to keep your domains and sites off blacklists and blocklists. For that, you need to know how a domain or site gets blacklisted in the first place. We identified some of the reasons:

- **Domain compromise:** Cyber attackers often attempt to take over popular websites to get to their owners' customers and clients, notably by using exploits or malware. If they succeed, they can turn affected servers or systems into bots that they then use for attacks. They can also inject spyware into forms, essentially making the sites part of their phishing campaigns. Some even inject malicious codes into pages, effectively turning them into malware hosts. If a site is compromised, it quickly gets included in blacklists or blocklists by antimalware providers and search engines.

- **Spamming:** Sending out unsolicited emails is considered spamming, and websites that users include in their spam folders little by little get flagged for the offense. Over time, these sites land on blacklists or blocklists maintained by antispam service providers and search engines, causing their senders to suffer email delivery issues.

- **Website visitor complaints:** Some website visitors are quite meticulous when it comes to scrutinizing pages for low-quality content, deceitful ads, and any other indicators of security threats. You would most likely get reported if they notice any of these on your website, possibly putting you on a blacklist.

- **Connection to malicious entities:** When a domain is known to have associations with malicious websites, it can also land on a blacklist. An example would be a domain that has an associated IP address that falls within an IP netblock with known suspicious websites. The innocent domain can very well become part of someone's blacklist as a precautionary measure. When that happens, it can lose precious website traffic.

All of the scenarios above can harm your domain's reputation. Now, say you ended up on a blacklist. What then? In most cases, un-blacklisting takes weeks. Site owners need to get rid of all ties to malware and malicious activities. Seeking those out, cleaning the affected systems and pages, and providing proof to blacklisters is a tedious and time-consuming process.

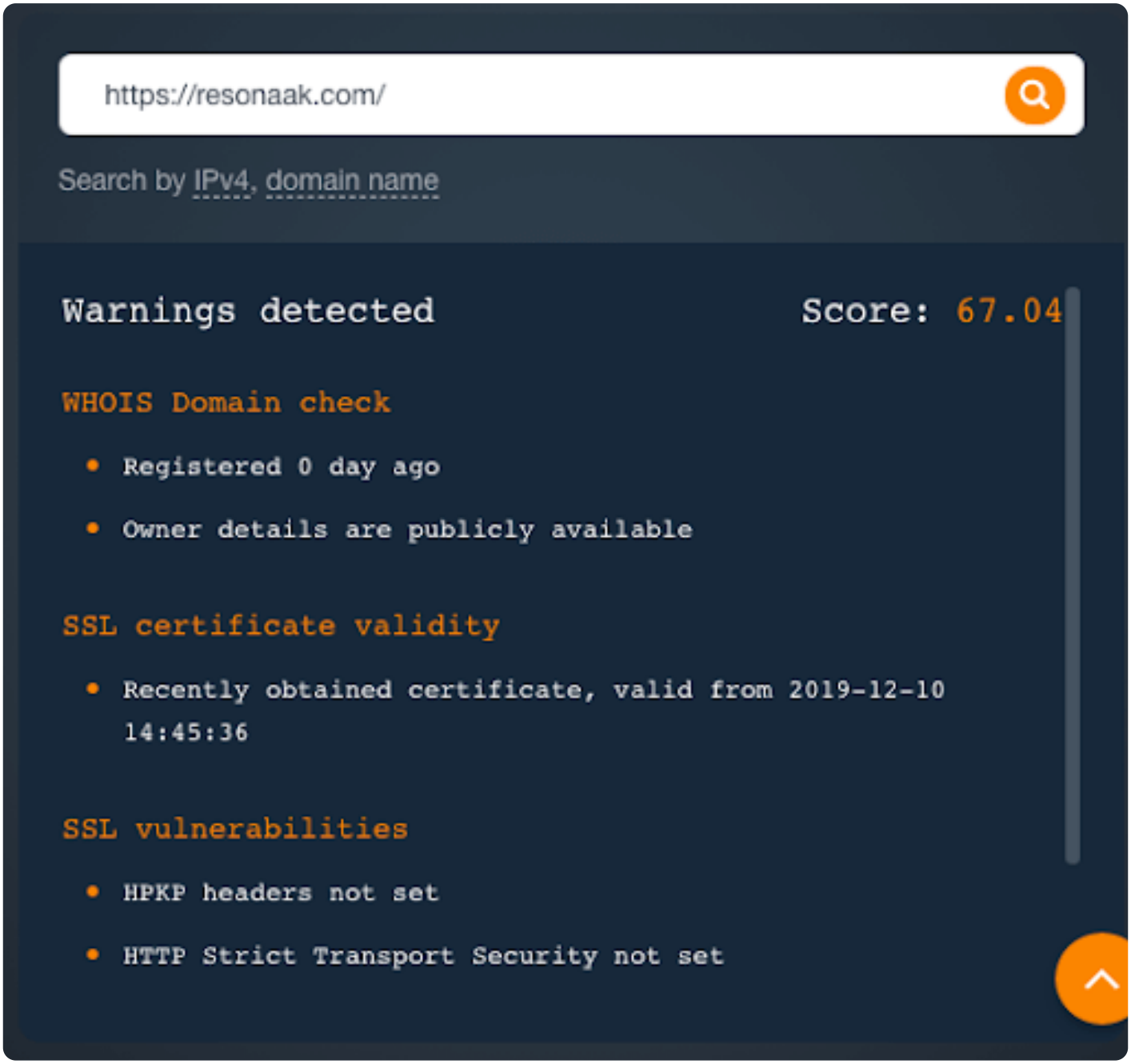
Avoiding the hassle altogether is a more practical alternative. Maintaining the security and reputability of your domain and sites is doable with the help of a **domain reputation lookup** tool like Domain Reputation API. Find out how in the following section.

How to Optimize Security with a Domain Reputation Lookup Tool

Robust domain monitoring is critical to avoid blacklisting. Organizations need to continuously be on the lookout for vulnerabilities that cyber attackers can exploit. They must make sure to properly configure all sites and their records (i.e., that they are not redirecting visitors to malicious sites or

the like). They also need to maintain threat-free pages. That is achievable with Domain Reputation API, as it can:

- **Help filter malicious domains and IP addresses connected to their network:** Screening the links published on your pages to make sure these don't point to malicious sites is a must. Integrating the API into your content management system (CMS) can help too. Every time a URL gets embedded in any content, you can run the API to make sure it doesn't point to a phishing site, for example. Running a suspected phishing site (from PhishTank) on the API would give a result like this. Given the site's low reputation score (the ideal is 100 to be considered safe to access), the fact that it is only a day old and has several Secure Sockets Layer (SSL)-related issues tells you that linking to it is not a good idea.



- **Help search for vulnerabilities:** The API can also be used to check whether your own domain has any vulnerabilities. The tool is an excellent monitoring application that security officers can use to check for issues that they have to address. For example, running a check of your domain may reveal that your SSL certificates are no longer valid. Then, you can

update them as necessary.

Strengthening your organization’s cybersecurity posture means finding proactive ways to keep threat actors out of your network. Screening everything that goes in and out of your network with the help of a **domain reputation lookup** tool like Domain Reputation API is one efficient way to do that.