Avoid Ties to Malicious Activity by Knowing the History of a Domain’s Ownership

Posted on February 6, 2020

While search engine optimization (SEO) experts often advise first-time site owners to use an old domain to gain instant authority on the Web, security professionals would caution that the practice can be risky.

That said, we do think there’s a way for site owners to enjoy the benefits of using old domains with as few risks as possible. In this post, we’ll tell you how knowing the **history of a domain’s ownership** by using tools like WHOIS History Search can help. But first, let’s take a look at why cybersecurity specialists may have reservations about using old or expired domains.

How Hackers Have Abused Expired Domains

Malvertising

A few years ago, it became standard practice for cybercriminals to use abandoned domains in malvertising campaigns. An example of this would be the case of oezelotel[.]com. It was first registered by denizduezguen@yahoo[.]de on 10 March 2014 to advertise various hotels. In 2016, it got parked since its owner did not renew its registration. Its historical WHOIS record showed that its ownership was transferred to domainmanagers@outlook[.]com on 4 June 2017. It changed hosts as well from a Germany-based server to a U.S. one and then began exhibiting malicious behavior.

A review of other properties owned by the same registrant indicates a penchant for going after expired domains and monetizing them via dubious ad networks. While a non-existent site may appear harmless, that is not the case. Abandoned or forgotten domains are often registered and “parked” to generate low-quality traffic (i.e., spammy links) to a major site.

Malware Hosting

Hackers have been known to go after expired domains from well-connected companies to lead their former users and practically anyone who knows them to malware-hosting sites. Such was the case of the abandoned domain of an advertising company, brentsmedia[.]com.

Its abandoned domain figured in a malware campaign that distributed the Angler Exploit Kit. Users who visited the domain and clicked a malicious ad landed on a fake site that automatically downloaded malware onto their computers.

Payment Card Credential Theft

Another example of an abandoned domain that inadvertently figured in a cyberattack was julierandallphoto[.]com. Like the others above, it didn't start as a malicious domain. It was a photography business site that the original owner put off renewing due to various reasons. It was then bought by a malicious user who put up fake online shops that sold branded merchandise at half their usual cost. Instead of getting what they purchased, however, customers weren't aware they were handing out their credit card credentials to the site's owner. Even worse, the new domain owner was using the original registrant's email address to communicate with clients of the fake shopping site.

While instances like these may not always make headline news, they do happen. They are also just some of the possible reasons why security specialists advise caution when considering the purchase of an old domain. We know that any ties to malicious activity can land a domain on a blacklist, but there are ways to avoid the hassle in the first place. One precautionary measure is to subject the domain of interest to a thorough background check before the actual purchase by using a tool that digs into the **history of any domain's ownership**.

How Can WHOIS History Search Help?

Knowing the **history of a domain's ownership** is crucial for IT personnel when helping their bosses pick the right virtual properties to buy. They can use tools like WHOIS History Search to scrutinize a domain's previous owners and their activities thoroughly.

A security specialist can run searches on the various domains that the company wishes to purchase to see if these have ties to malicious sites or are tagged for violations and thus part of blacklists. For instance, if a domain you want to purchase previously figured in a phishing scam, it may still be part of a blacklist. As such, despite its current authority due to age, potential customers may still not be able to reach it because it may be blocked from their end.

It is thus worthwhile to subject every domain on a company's to-buy list to an in-depth background check. After obtaining a list of its previous owners, registrars, and organizations from WHOIS History Search, you can run it through a domain health check with tools like Threat Intelligence Platform. This step may reveal open ports that are prone to hacking, unpatched vulnerabilities that can be exploited, dangling records that can be abused, as well as redirects and malware presence.

In an age where their online presence primarily defines organizations, it is indeed worthwhile to heed and abide by SEO best practices. Then again, they must not forget that a cyber attack occurs every 39 seconds. And so, while landing on the first page of search engine results can be done faster by using old domains, these must be ones that do not have a checkered past. Potential owners of expired domains can rely on tools like WHOIS History Search to get a complete history of each domain's ownership so they won't get less than they bargained for.