Enriching Domain Protection Through Historic and Reverse WHOIS Data Monitoring

Posted on September 11, 2019

The foundation of a domain's existence on the Web is its credibility. It must be secured at all costs because it's constantly under threat from malicious elements that are out there staging. As such, **domain protection** is an indispensable component of overall cybersecurity efforts because not just business viability but a domain's very own survival is at stake.

A company can protect its domain in different ways. For one, it can initiate its own in-house solution which would require substantial expertise and investment to put in place. Another option is to delegate the responsibility to experienced specialists dedicated to providing brand and digital protection services.

As part of their services, such companies track and analyze potentially dangerous domains that use the keywords associated with their clients' organizations or brands. However, such a monitoring function requires unimpeded access to the available data on both recent and historic domain registrations. It may sound easy for some, but not all companies providing **domain protection** services have that capability. Let's take a closer look.

Access to Huge Amounts of Data Is a Must

As **domain protection** teams are constantly on the lookout for existing and potential threats to their clients' domains, they mostly rely on access to open-source domain data to monitor dangers promptly. This could be quite a challenge considering that there are now hundreds of millions of active domain names and billions of historical records to sift through.

For a team to avoid potential attacks and investigate existing issues, it must tap into huge amounts of domain data on gTLDs, ngTLDs, ccTLDs, etc. in order to ensure precise results. That data must also be well parsed and available in easily readable formats in order to minimize, if not eliminate, any additional workload on the client's behalf.

Proprietary Tools for Data Enrichment

WhoisXML API has been in the cybersecurity sphere for more than a decade with a verifiable track record. Building on this, we now offer our clients a data enrichment service with our

comprehensive **domain protection** solutions — which include WHOIS History API and Reverse WHOIS API proprietary monitoring tools.

Our WHOIS History API allows you to dig deep into a domain name's past to discover any history of malicious activity. Virtually nothing can be hidden from our historic databases which contain more than 300 million active domains, one billion historic domain names, and over 5 billion historical WHOIS records, which have been compiled and constantly updated since 2008.

Reverse WHOIS API, on the other hand, permits you to search for domain records using specific terms — parsing through hundreds of millions of domain events of today and the days before. A query can be created with search terms such as name, email, phone number, address, etc. In turn, the API will generate a report of any other domains registered now or in the past and share your specified data point. This enables you to discover all the domains that are associated with your current investigation to reveal dangerous connections, potentially identifying evidence of malicious networks.

Both APIs can be used separately or, better still, complement each other to find out everything about an entity of interest. Combining them can uncover more details relevant to the keyword being looked into or the organization conducting the query.

Let's take a look at the steps involved in such an investigation:

Step 1 — Tracking connections through Reverse WHOIS API

```
{
    "apiKey": [redacted],
    "searchType": "current",
    "mode": "purchase",
    "basicSearchTerms": {
        "include": [
            "Airbnb, Inc.",
            "US"
        ],
        "exclude": [
            "Europe",
            "EU"
        ]
    }
}
```

Request body sample

```
{
   "domainsCount": 2,
   "domainsList": [
        "airbnb.app",
        "airbnbhost.app"
    ]
}
```

Sample output in JSON format

Reverse WHOIS lookup requires the input of a specific search term in the WHOIS database. As noted earlier, a query can be made using specific attributes such as name, email address, phone

number, registration date, or any information detail that is usually included in a WHOIS record.

The term could be an exact match or a ‘fuzzy’ match such as inputting a common name, like Peter, or searching for email addresses that contain a particular term like ‘abc’. You can also filter your results to search only for records that correspond to a specific month or year.

Whatever term is used, the query will result in all the domain records — both current and historic — that correspond to the specific term inputted, well parsed and easily integrated into existing systems.

The result produced can be used to check if the keyword appears in WHOIS or registrant details of other domains and, therefore, can help verify if all the domains in the list are familiar to you or your client — registrant details are often spoofed by cybercriminals for phishing or other malicious purposes.

Step 2 — Searching the past through Historic WHOIS API

During step 2 the domain results that were obtained from the first step are run through the WHOIS History API which, in turn, can produce results that are available in PDF format.

At this stage, it is important to pay attention to certain details to determine if the domains being investigated are legitimate or not. For example, registration details must match the infrastructure of the domain being analyzed. Otherwise, it could point to malicious activity.

Importantly, for companies obtaining data for **domain protection** activities, using WHOIS History API is preferred over WHOIS API because the former can turn up data that may have already been updated in the current database. For example, historic WHOIS can track down domain owners from the time the domain was first registered even if the current details have already been concealed or changed, thus providing deeper actionable intelligence.

Best of Both Worlds

The two-step investigation involving WHOIS History and Reverse WHOIS APIs underscores the advantage of having access to all the available tools to allow cross-checking and data enrichment. The approach strengthens the delivery of **domain protection** services by cybersecuritycompanies.

Reverse WHOIS API can immediately dive into specific search terms to set the focus of the investigation as well as can be used separately to combat brand infringement. The data obtained can then be verified or corroborated using WHOIS History API, reaching records that may not be currently accessible but can hold the key to the immediate implementation of **domain protection** solutions.

Safeguarding a domain from threats requires huge amounts of data plus the tools needed to efficiently access, monitor, and analyze them in order to identify potential risks. Partnering with an experienced cybersecurity provider such as WhoisXML API can help ensure better and richer **domain protection**.