How to Conduct a Website Domain Search for Cybersecurity Purposes

Posted on June 29, 2020

WHOIS lookups are a viable way for cybersecurity professionals to analyze domains' integrity. Though they may seem less exciting than, say, deploying some nifty pen-testing tools, WHOIS lookups remain useful as a first step in catching threat actors.

In fact, identifiers in WHOIS records can clue investigators in on a domain's past usage and allow them to pinpoint indicators of compromise (IoCs) residing within their networks. With WHOIS data, they can also identify domain associations and effectively map attacks that happened or could happen on their infrastructure. Read on to learn more about why conducting website domain searches is critical to your digital operations, and how WHOIS API and WHOIS Lookup can facilitate it.

Why Perform a Website Domain Search

WHOIS lookups support a variety of cybersecurity processes such as:

Threat Intelligence Gathering

Examining a domain's WHOIS records allow cybersecurity professionals to better understand domain-related alerts from security information and event management (SIEM) and security orchestration, automation, and response (SOAR) solutions so as to pinpoint which ones require immediate attention. Certain WHOIS records can help provide context to IoCs found within your network, speeding up detection and incident response.

DNS Forensic Analysis

WHOIS records enable experts to discover the name servers associated with domains so they can effectively analyze the corresponding Domain Name System (DNS) records. A domain's WHOIS record also allows seeing what changes have been made and when, in order to better study the timing behind an attack and related events.

Domain Name Analysis

Analysts often rely on WHOIS records as a primary data source for white papers, reports, and other resources. Security researchers can use a WHOIS database as well to spot registration trends across generic (gTLDs) or country-code top-level domains (ccTLDs). They can also uncover the following domain trends by using WHOIS data:

- The dominance of a particular TLD across registrants, organization types, or countries
- The modal length of domains (i.e., how many permissible characters there are in a name)
- Possible combinations of characters, numbers, and symbols in domains
- Frequency of individual letters or pairs of characters

These are just three notable use cases of WHOIS records. Other practical applications include assisting in domain name transfers and brand disputes. In that case, WHOIS records can function as a phonebook. This “phonebook” was the original idea behind the whole WHOIS system—to identify physical entities behind a domain and provide their availability. Note that certain new data protection rules like the GDPR have impacted one’s ability to do so since many WHOIS records are no longer publicly available.

Still, WHOIS remains the only official source of this kind of domain data. Users can refer to it to obtain administrative, technical, and abuse contact details. And if they don’t receive responses, users can reach out directly to the domain’s registrar for assistance. The registrar details always appear on records, even for privacy-protected domains.

How to Use WHOIS API for Website Domain Searches

Cybersecurity researchers can integrate WHOIS API into their existing security architecture. Another alternative is to run the API using the command-line interface (CLI). Users can also opt for the API's web version, WHOIS Lookup, if they don't have a programming background.

By entering a domain, email address, or IP address into the API, users can obtain the associated WHOIS record. Let's take a look at an example.

We chose to investigate the URL http[:]//www[.]4celia[.]com/wp-admin/2z8/ that points to a command-and-control (C&C) server for the Emotet banking Trojan. Emotet spreads via email. It takes the form of a macro-enabled document. Once executed, the malware attempts to contact any of its C&C servers.

We ran the domain 4celia[.]com on WHOIS API, which revealed its registration details:

```
"createdDate": "2019-12-07T10:43:57Z",
"updatedDate": "2020-01-28T09:09:10Z",
"expiresDate": "2020-12-07T10:43:57Z",
"registrant": {
    "name": "john tuza",
    "organization": "centatech",
    "street1": "Makerere university",
    "city": "kampala",
    "state": "kampala",
    "postalCode": "256",
    "country": "UGANDA",
    "countryCode": "UG",
    "email": "johntuza94@hotmail.com",
    "telephone": "256785958670",
```


The result shows that the domain was created in December 2019, exactly a month after security

researchers saw a sudden spike in Emotet-related spam. The domain will soon expire, though, which is expected as hackers don't hold on to domains for long to evade detection.

You may be wondering why the domain's ownership details are not privacy-protected like those that figure in high-profile attacks. A possible reason is that the domain is legitimate, but the attackers managed to compromise it.

Another reason is that the record contains forged details or somebody else's information is being misused. For instance, Makerere University is indeed an existent organization, based in Kampala, Uganda. John Tuza also seems to be a real person and presumably was a student at that university.

However, the registrant's organization, CentaTech, isn't headquartered in Uganda. According to its Facebook page, CentaTech is based in Vancouver, British Columbia, Canada. Still, that may not necessarily be true. The registration location for its official domain centatech[.]com says that a Nepal-based user reserved it, as is shown below.

```
"registrant": {
    "organization": "Home",
    "state": "Bagmati",
    "country": "NEPAL",
    "countryCode": "NP",
```


In addition, a google search containing the terms "Makerere centatech" returns 4 results altogether (at the time of writing), all about the malware relation of this very domain.

This exercise demonstrates how WHOIS records can provide researchers with a starting point for investigations. Analysts can formulate theories based on the details in a domain's WHOIS record. Falsities and mismatches in information can also be signs of malicious intent.

Performing website domain searches for addresses you own or find in your logs allows you to keep track of their state, changes, and usage. By screening domains with WHOIS API, infosec professionals can safeguard their networks from destructive breaches in the long run.