On the Way to a Safer Internet: 5 Tough Challenges to Overcome with WHOIS API

Posted on January 23, 2019

Just like in the real world, the Web is composed of good and bad places and people. Thus, to avoid the wrong districts and the malicious agents that reside there, companies need the right cybersecurity workflows in place — especially as digital systems are taking over businesses.

However, is it possible to stay away from dangerous hosts and websites like you would sidestep shady neighborhoods? It is, which is why including a domain data protocol like WHOIS makes sense. But first thing first:

What Is WHOIS?

WHOIS is the address book of the web. It's a repository of records that contains details about domains' owners, history, important dates, and other facts. Authorities and interested stakeholders can use that data as it is or link it to other sources of information for a variety of purposes which are further explored in this post.

What Is WHOIS API?

As an interface, WHOIS API tackles the key limitation of WHOIS as a data source: its disintegrated form. It takes a lot of time to go through each record individually, particularly, as thousands of new domains are registered on a daily basis. WHOIS API, on the other hand, allows you to easily get access to data points through feeds and integrate these with existing applications through major programming languages.

Why Is WHOIS Important?

Here are 5 of the tough challenges that cybersecurity specialists and professionals can overcome by using WHOIS data.

1. Identifying Cyber Attackers Before They Strike

Cybercrime is on the rise, and what's worse is that it could reach stakeholders related to any company and cause irreversible damage. In April 2018, a phishing incident affected 128,000 patients of New York Oncology Hematology, in which victims were deceived into entering their passwords onto a legitimate-looking page.

Attacks like these are becoming more sophisticated and difficult to detect as part of normal company operations. So what's the alternative? IT departments can take a proactive stance by applying threat hunting principles and futureproof their organization — enumerating possible situations and taking measures to be steps ahead of attackers.

To support threat hunting techniques, WHOIS feeds and DNS protocols provide information about newly registered domains and other details like owners' contacts — thus possibly spotting phishers. Additionally, if investigators receive tips about a specific bad actor or a group of criminals, checking WHOIS records for suspicious websites can help as there are usually identical patterns across registrations performed by a similar entity.

2. Investigating Cybercrimes

It's getting harder to identify and prosecute cybercriminals, and pressure constantly mounts on authorities as they fight organized groups around the world.

Law enforcement agencies need to keep up and apply creative approaches to outdo perpetrators. For instance, in its attempt to unmask a cybercriminal, the FBI once created a fake FedEx website.

But more often not, the technique of impersonating online assets is used by fraudsters to steal valuable information, and cybersecurity investigators who pay attention to domain information can spot forged online entities via their WHOIS records — accessing verifiable data on websites quickly.

3. Facilitating Domain Activities

More and more domain names are registered, transferred, and managed every year. There were 339.8 million domain name registrations across all top-level domains (TLDs), as of the second quarter of 2018. For sure, those in the domain business need to grasp and sort domain data well.

Domainers must stay updated about expired, deleted, and available domains in real time and they can use **WHOIS API** to identify investment prospects proactively, rather than finding out late that a domain of interest was for sale again.

Registrars, as well as the rest, need a WHOIS protocol, notably for the yearly review of registrants' contact information as required by The Internet Corporation for Assigned Names and Numbers (ICANN), or to ensure the security of domain ownership transfers.

4. Preventing Online Transaction Frauds

Digital money transfer service Venmo has recently suffered payment frauds that led to $40M in losses, partly because of scammers executing fraudulent bank transfers. Many times, such fraud incidents could have been prevented had companies implemented the right measures — one of which is guaranteeing identities.

Let's say you are in charge of reducing fraud level for the services offered by your company. You might use WHOIS' data points to monitor the change of email addresses in user profiles. If the new domain used for contact was only registered recently, this might be a red flag to watch out for.

Has a hacker switched the email address of a legitimate customer for his instead? Does he now have the right to alter or divert payments? To be sure it's not the case, you could set up a WHOIS verification process before accepting changes that could put you at risk.

5. Combating Domain Name Infringements

Domain infringement is being increasingly scrutinized. The number of .uk addresses suspended

because of it doubled in 2018, for example. So, in a nutshell, how do infringing activities take place?

Cybersquatters, among others, bypass trademark rights and register country code top-level domains (ccTLDs) names in the hope of receiving compensation from the legitimate owners who have been slow at securing addresses as part of their business expansion plans.

WHOIS API can help avoid this and make companies more responsive. In fact, monitoring multiple domains for aspects such as date of registration allows flagging instances of cybersquatting — i.e., by comparing it with trademark registration dates to see which one came first.

On top of that, companies can monitor domain registrations to detect fraudulent entities that attempt to associate themselves with their brands, including deliberately misspelled brand names and corresponding domain addresses that cause confusion.

WHOIS help raise security standards across countries. It is available for all, and its access is made more efficient with WHOIS API and the comprehensive database that empower data feeds.

Do you want to see how WHOIS can contribute to streamlined cybersecurity efforts? Contact us at general@whoisxmlapi.com to get more information and schedule a demo.