WHOIS Database Download:
5 Newsworthy Use Cases

Posted on March 7, 2019



Organizations are better aware of the informative value of domain names — .com, .edu, .org, and many others. That's imperative in today's global business environment, where a significant share of operations occur on the Internet while cyberattacks, brand infringements, and more mishaps haunt the place.

This is where we put the spotlight on domain data, because what's a website without its domain name? A site can alter elements like headlines, subheads and content, but never its domain name.

That's why WHOIS databases are worth talking about since they contain a comprehensive list of domain names, consisting of a rich network of data on websites and the people behind them.

In fact, to cull accurate information from the vast possibilities out there, many professionals use our solution WHOIS Database Download as a part of their investigation. The records which are traced, compared, and connected to other data can then reveal adequate details about unfamiliar entities. Here a few specific use cases.

1. Reinforce Threat Hunting Techniques

No one is immune to cyber threats that could catch even the most powerful institutions off guard. In fact, a hacker attack happened at the Ministry of Economic Affairs not long ago, resulting in the website shutdown.

In order to avoid such incidents and establish their own offensive mechanism, companies can follow threat hunting practices to identify attackers before they act. That's possible since criminals lurking near organizations often have particular behavioral patterns, notably, in the way they register domains.

Here is where threat hunters take advantage of domain-related data. To enrich their intelligence, they may work with a WHOIS and DNS protocol applying different search strategies, from integrating automated feeds to customizing searches where users can look for specific owners' contact details, including registration and expiration dates.

2. Accelerate Incident Response

Timely response to attacks is not easy yet crucial, and it could be a company's salvation from financial, operational, and reputational harm.

On average, an incident response takes 61 days from occurrence to discovery; 8 days from discovery to containment; 40 days from the engagement of forensics until the investigations are complete; and 41 days from discovery to notification. Imagine the system damages and corresponding data loss that could occur during that period.

To swiftly react when cybersecurity incidents occur, security information and event management (SIEM) is a measure that companies opt for, and WHOIS key points can fuel that process by adding details about domains and giving more context to detect, analyze, and respond quickly to spotted anomalies.

3. Facilitate Threat Intelligence Efforts

Cyber attacks won't stop in the years to come, and while companies are in the loop about it, many still don't toughen their security. In 2018, 67% of SMBs experienced at least one form of cyber attack. But what can they do? Threat intelligence, a proactive approach applied by companies might just be the way to go.

Through that practice, experts are able to develop full-fledged layers of security, not just to comply with security standards but also to counter future threats — e.g., by checking the hosts' infrastructures, extending the analysis to third-party connections as well as identifying system vulnerabilities. Amid the array of tactics, WHOIS and DNS data can be connected and automated via TI feeds to study peculiar recent and offshore registrations.

4. Prevent Cybersquatting

Cybersquatting is the act of purchasing lots of top-level domains illegitimately and carrying out shady tactics, often for profit. Not only do squatters expect to financially benefit from reselling domains, some may also have darker intentions and publish malicious or misleading content that will taint the domain's history.

Just recently, Chicago Blackhawks took part in a cybersquatting dispute to win Blackhawks.com — which was owned by someone else making no legitimate use of it. Things went well for the hockey team, which ended up winning the domain as the squatter did not build a defense against the claim made.

To resolve domain squatting issues, WHOIS can provide domain ownership, allowing claimants to put their hands on telephone numbers, emails and physical addresses to contact the entities behind a domain or just go straight to the relevant authorities.

5. Monitor Contractors

Third-party company connections can be exploited by hackers as entry points for attacks. Indeed, a third-party data breach exposed the information of job applicants, compromising highly sensitive details including their social security numbers. Thus, before entrusting others with Web-based services or affiliations, it is always prudent to verify their credibility.

Businesses can rely on **WHOIS databases** to examine others' reputation by searching domains to find their history of ownership, registration, and expiration information. Legitimate websites seasoned in the industry are more likely to contain credible information such as owners searchable as real persons and no prior connection to known malicious domains.

It is difficult for companies to tell what is happening with websites and domains when they are not sure where to look in the first place. The Internet is supposed to be a platform where users can investigate shady entities if they need to, and WHOIS databases provide the necessary informational backup.

Would you like to find out more about what WHOIS Database Download can do for you? Reach out to us at support@whoisxmlapi.com.