How Authorities Can Clamp Down on Cybercrime with Bulk Domain Lookups

Posted on May 29, 2020

Nominet's takedown of 28,937 malicious sites is a small triumph for law enforcement and other internet stakeholders. With help from authorities, the domain registry has been on a quest to purge the .uk namespace of rogue domains since 2009. Now, for the first time in five years, the total number of suspended domains has finally reflected a decline. The figure may not seem like a lot, considering that it only accounts for 0.22% of the 13 million domains registered in the U.K. Still, it was a milestone for an industry fraught with prolific bad actors. In the U.K. alone, an average of 800 cyber attacks per hour hit councils. This number translates into around 263 million in just half a year.

Curbing cybercrime is an essential undertaking for internet authorities, in light of new digital technologies, and the Internet's evolving business model. Unfortunately, lack of resources at both the domain level and cybersecurity know-how, as well as legal barriers, slow down authorities in their efforts to hunt down perpetrators. This can be made easier, though, with a bulk domain lookup solution.

Bulk WHOIS API is a good example of a research tool that cyber investigators, electronic crime units, and regulatory agencies can rely on to faster inspect a significant volume of domains. With an IP address, email address, or domain name, users can obtain pertinent registrant information for a group of web addresses. Let's take a closer look at how users can get more out of the solution.

How Bulk Domain Lookups Help Authorities Mitigate Cybercrime

What makes Bulk WHOIS API compelling is that it slashes the time investigators spend on identifying indicators of attack (IoAs) and threat actors' other resources. By filtering results based on an individual or a company's name, a domain, or an IP address, users can quickly obtain the WHOIS record details of offending hostnames. Such records include the registrant's name, organization, email address, registration location, registrar details, and domain age, among others.

Bulk WHOIS API can help explicitly with the following:

1. Establishing Relationships between Domains and Known Criminal Networks

Attackers do a great job hiding their tracks by means of secure websites, proxies, covert communication channels, and sophisticated software. Yet crafty as they may be, they still leave digital footprints. Signs of ongoing network intrusions, for instance, include off-hour malware alerts and unfamiliar servers communicating with internal hosts. All these may leave a trail in the form of IP addresses or domains.

These data points can help the authorities look for more information via Bulk WHOIS API. The program provides law enforcers with a starting point for their in-depth investigations to track down the culprits' identities. They can also update their internal databases with new indicators and attacker profiles using the WHOIS data obtained from the solution.

2. Aiding in Namespace Cleanups

Agency departments, such as the Federal Bureau of Investigation (FBI)'s Internet Crime Complaint Center (IC3), and nonprofit organizations like the Public Interest Registry (PIR) collect complaints, examine cases, and compile victim profiles. It is also their mission to get law enforcement involved in the cases.

Still, with thousands of cases filed every single day, the weighing factors may prove challenging. That is where Bulk WHOIS API come in handy as it allows concerned parties to retrieve the WHOIS records of multiple illegitimate domains in one go. With it, users can streamline their process of validating complaints and gain more insights into how domains figure in attacks. As a result, registries can take action on suspicious domains promptly.

3. Facilitating Other Internal Processes

Law enforcement agencies often lend their expertise to internal divisions and similar groups that police the Internet. They can use Bulk WHOIS API to obtain threat intelligence for cases, analytical

research, and digital forensics. The program allows users to gather threat data for consolidation, refinement, and cross-referencing across multiple systems.

What Happens Next?

Law enforcers can request registries to suspend malicious domains after proving their ties to criminal activities with a bulk WHOIS lookup program. They can also request court orders to expand their e-discovery and other data aggregation initiatives. In addition, they can forward the WHOIS data to the appropriate agencies so they can deal with the matter.

In most cases, threat actors commit criminal acts in countries that can't prosecute them. Authorities can coordinate with international law enforcement agencies, such as the International Criminal Police Organization (INTERPOL), the European Union Agency for Law Enforcement Cooperation (EUROPOL), the Gulf Cooperation Council Police (GCCPOL), or the ASEAN Chiefs of National Police (ASEANAPOL) to timely respond to attacks.

Stewards of the Internet, such as law enforcement agencies, can depend on bulk domain lookup solutions like Bulk WHOIS API to pursue cases against cybercriminals and rid the Web of malicious sites. With Bulk WHOIS API, watchdogs can effectively remove unwanted sites from the public domain, thus ensuring the safety of society at large.