# Monitoring Newly Registered Domains

Posted on October 11, 2018

The first line of defense for companies that want to protect their staff or customers from bogus websites is monitoring domain names.Hackers will use variations of domain names to lure unsuspecting users onto portals whose purpose is to steal private information and drop viruses onto devices.

Whois XML API offers a Domain Research Suite that provides users with the ability to watch whether new domain names closely resemble existing registrations, which may be intended to trap internet users.

## Why Monitor New Registrations?

There are a variety of use cases where information on newly registered domains can be of interest to particular individuals or businesses. Web development companies can utilize these lists to prospect for new business. Similarly, marketing companies can use the registration information to build email lists.

Monitoring new registrations is particularly useful for security professionals. Hackers often register new domains to perform cyber attacks. Therefore, a new domain monitoring alert could play a vital role in a proactive security solution.

## The Bad Guys Register Too

Hackers, like all other Internet users, need domains for their online operations. Carrying out web-based attacks using a domain name provides the hacker with much more flexibility than a fixed IP address. For example, if an attacker has set up a Distributed Denial of Service (DDoS) attack, they may need their proxies to acquire commands from a specific web address.

By utilizing a domain, they can rapidly change IP addresses and servers without needing to update any client settings. This flexibility allows them to avoid any defensive measures. It can also help the hacker evade the authorities, especially when the malicious servers and DNS services fall outside of their jurisdiction. There are a few other nefarious reasons for registering domains, such

as utilizing them for phishing campaigns.

## Gone Phishing

A phishing campaign requires an unsuspecting user to click on a malicious link. If the link resembles the domain of an existing organization, the chances of successfully deceiving the user increase substantially. It is therefore imperative that businesses remain vigilant of any registration which closely matches their legitimate business name to defend against this type of attack.

When identifying a potentially malicious registration, a WHOIS query can quickly inform infosec professionals of its legitimacy. This record listing provides a treasure trove of data about the domain owner, which includes their contact details, the creation date, and which servers host the domain's records.

## The Best Defense

The Whois XML API's Domain Research Suite offers a set of tools that automatically report whether a registration that has appeared in the Whois database of registrations may be of questionable intent.

For instance, the Domain Monitor API watches out for companies that users specify they find of interest. Whenever the Whois record for the registrant changes, Domain Monitor sends an email alert to analysts about what security professionals may consider suspicious activity. Cybersecurity staff receive details of any changes that have occurred for criteria they have used to filter the registration, including: the Updated Date, Created Date, Expiration Date, Registrant Information, the Domain Status, and more.

Hackers also tend to follow brands to piggy-back on the popularity of products and services. offers a Brand Monitoring Tool that reports on exact and fuzzy matches of brand names. The tool will report on variations and common misspellings of keywords. The API alerts users when it returns keyword matches that reveal domains which either are newly registered or have recently expired.

Some hackers have developed reputations or even profiles that enable infosec professionals to

keep tabs on their activities. The Registrant Monitor Tool alerts cyberdefense specialists of all Whois database registrants who have newly registered, deleted or modified domains. The API uses keywords based on the names of individuals or companies that white hats want to track. The tool sends alerts when the tracked names register new domains. The API even offers a report of when target names have updated existing domain registration information or any of their domain names expire.

Whois XML API offers dozens of tools to aid infosec professionals in the defense and forensics work of foiling bad actors. Domain Monitor API, Brand Monitoring Tool, and The Registrant Monitor Tool all provide organizations and individuals with effective protection where it counts most: before hackers can strike.