5 uses of Whois data for Cyber Security Professionals

Posted on January 25, 2016

2015 saw a major surge in Cyber Crime; right from an increase in criminal activity, to the scale of the crimes and lastly the innovative techniques of crime that are being adopted by Cyber Criminals. Cyber Security professionals from across the world have rolled up their sleeves as they are well aware that this New Year is not going to be a cakewalk, at this rate. The emphasis, for them, now is shifting to being proactive and preventing attacks instead of reacting to the crimes.Here is our list of 5 ways in which WhoisXmlApi.com can be used to help prevent Cyber theft this year and try to make it a joyous time for everyone; except for the Cyber criminals, of course!

1) To identify malicious websites

A domain record can be a very handy preliminary point to figure whether a website is potentially harmful, and/ or may be involved in any case(s) of Cyber theft. A lot of factors can raise red flags, following which further investigations can be undertaken by Cyber security professionals. Some of the important elements to be noted are:

- A fairly recent registration date of the domain
- A fairly close expiration date of the domain
- Registrant from a high-risk country
- The registrant and company address being in different locations

These are some important commencement points, based on which a professional can take further steps to stop any malicious websites from duping people. Also, they can identify other sites and

networks that are associated with the concerned site and can shut them, if needed.

2) To identify fraudulent entities

The Reverse WhoisXmlApi search can help Security professionals in finding domain records for a particular search term(s). Thereby, a broad search can be focused on a limited data and all the corresponding details can be availed. A query can be made on any term(s) used in the Whois Record, like:

- Individual's name
- Company name
- Email address
- Phone number
- Address
- Any other parameters covered in a Whois record

Once the domain records are returned, professionals can find out various domains and operations corresponding with the query term(s). This can help keep a check on nefarious activities from a single source.

3) To identify different associations for a fraudulent activity

With the help of WhoisXmlApi.com, Cyber Security professional can find all the domains, websites and IP addresses associated with a particular (or even a series of) fraudulent activity. Various data combinations can be used to draw a link. For instance, linking an email address to other maliciously flagged websites, linking address to other maliciously flagged websites etc.These associations can be identified by using:

- WhoisXmlApi search

- Reverse WhoisXmlApi search
- WhoisXmlApi Domain IP database search

Data from these 3 sets of Whois records need to be cross-matched to find various common linkages by professionals and further steps can be taken to curb their activities. Also, this data is used to monitor domains, IP addresses, name servers and registrant information of suspect characters to prevent future Cyber thefts.

4) To identify fraudulent domains with DNS (Domain Name System)

Timely DNS tracking can be an important key in helping prevent Cyber theft. A query can be made on an IP address and the search will return all the domain records related to that particular IP. If a fraudulent domain is found, its IP can be tracked and all the other domains that rest on that IP can be verified by professionals and appropriate actions can be taken.Cyber security professionals usually cross-reference domain names in the Whois data with other useful DNS data points to get more accurate and correct information.

5) To identify credit card fraud

While registering for a credit card, Security professionals can do a background check on the email address provided and malicious email address can be flagged. By doing so, huge losses can be prevented by companies issuing credit cards.

The well parsed, consistent and accurate Whois records from WhoisXmlApi.com can act as a great start for Security professionals to keep a check and deter Cyber theft.

In case you need Cyber Security solutions or any further details to prevent Cyber Crime for your company, do write to us at general@whoisxmlapi.com and we would be happy to help.