IP Geolocation Finds Hacker Origins of Attack

Posted on October 3, 2018

Cyber attacks and data breaches make the news on a regular basis. However, with over 50% of U.S. businesses experiencing some form of cyberattack in 2017 alone, the scale of the problem is much larger than the fraction reported by the media. Organizations of all sizes and in every industry are under constant attack, but who is behind these cyber assaults and where are the perpetrators located?

It is essential to understand the origin of a cyber attack and to find who is responsible for it. Not only can this evidence help bring cybercriminals to justice, but it also assists defenders with the information they need to prevent similar incidents from reoccurring.

Whois XML API offers several software applications to help cybersecurity and law enforcement authorities identify the geographical location of IP addresses. Tools like Reverse DNS API and IP Geolocation API in combination quickly zoom in on the whereabouts of the domains that security outfits have identified as malicious.

The Main Culprits

While Whois XML API affords tools that reduce the time it takes to find the point of origin of malevolent domains, hackers develop their own security tactics. Black hats don't make finding their identity or location easy. According to an Akamai study in 2014, the majority of cyber attacks originate from China, with the United States coming in second, closely followed by Taiwan, Turkey, and Russia.

However, organizations should not take these statistics at face value. Hackers cover their tracks by using proxy servers, Virtual Private Networks (VPNs) and other compromised networks. For example, a Latvian attacker could use a proxy server located in Brazil to assault an organization in Nigeria. That example shows why attributing an attack to a specific site or domain is so complicated. To truly uncover the identity and location of an attacker, investigators have to utilize a combination of forensic techniques.

Building the Supporting Evidence

Over and above the originating IP address used in a cyber attack, forensic investigators also scrutinize the files and data attackers leave in their wake. By analyzing evidence such as the grammar embedded in software code and the metadata in any discarded malware, investigators create a digital profile. Using this collective evidence, they are then able to identify the possible perpetrator.

However, even though attributing an attack involves several investigative techniques, the originating IP address or domain remains a crucial piece of evidence. Submitting this information to blacklists and reputational databases can help organizations prevent attacks from locations which have previously been identified as attack vectors.

Putting the Geolocation Tools to Use

The Whois XML API Reverse DNS API tool will reveal the domain name of any IP address. A reverse DNS lookup will also disclose the region where the server of the IP address is located. Apart from that, cybersecurity teams use IP Geolocation API to get more specific location information.

The IP Geolocation API uses Whois XML API's proprietary Geo IP database to identify the physical location of visitors to a website. The database accounts for 99.68% of all IP addresses used worldwide. The API narrows geographical information down to the latitude and longitude, time zone, country, region, city, and even ZIP code. The data the API provides enables companies to block any visitors trying to access their websites anonymously. The tool delivers data to allow security personnel to compare visitors' locations with the available customer data to prevent online fraud and possible identity theft.

Hackers can now work from any location in the world. They are able to attack websites and set up malicious domains with impunity. Infosec and law enforcement authorities can stay one step ahead of bad actors by arming their organizations with the sort of geolocation weapons that Whois XML API has to offer.