Find Out More About an IP Address via WHOIS Lookup and WHOIS API

Posted on July 13, 2020

IP addresses are unique identifiers for devices hooked to the internet. These addresses, which are represented by numerical values, allow computers to communicate over the Transmission Control Protocol via IP (TCP/IP). The protocol routes users looking for Internet-connected hosts or websites to the right destinations using IP addresses as a reference.

However, notably because of inherent design flaws, attackers can spoof IP addresses with the intention of, for example, misdirecting users to dangerous sites. For this reason, among others, it is critical to routinely scan IP addresses passing your network filters to ensure their integrity and identify any potential links to malicious campaigns or networks.

As part of this process, it is possible to do an IP lookup via WHOIS Lookup and WHOIS API to extract the ownership details of a given address for further inspection. What's more, both products permit gathering all sorts of relevant details such as if an IP address hosts a domain and which regional Internet registry (RIR) manages the resource.

Why Run an IP Address WHOIS Lookup?

Let's take a closer look at some use cases of an IP address WHOIS lookup.

1. Fraud Detection

Authorities can stay hot on the trail of criminals by tracking the origin of their IP addresses. Fraudsters paying for purchases using stolen payment card information are also identifiable based on the IP addresses logged in when they made orders. Investigators can first acquire the suspicious IP addresses from the merchant's website and payment processor. Then they can run the IP address on WHOIS Lookup or WHOIS API to obtain the name and contact details of its owner and connected domains if any.

2. DNS Forensic Analysis

WHOIS Lookup or WHOIS API can enhance the data gathered from open-source intelligence (OSINT) databases to more comprehensively analyze IP addresses that are attempting to

establish connections with their systems.

In the wake of a malware attack, for example, you can use the said sources of intelligence in an attempt to establish whether or not your network might be making or receiving calls to or from any known command-and-control (C&C) servers by screening the IP addresses recorded in your logs. Users can also integrate the API into a network filtering tool for more timely detection of rogue IP addresses.

3. Spam Blocking

Email reputation services and the DNS-Based Blackhole List (DNSBL) closely monitor suspicious senders that figure in spam campaigns. You can augment the effectiveness of such services with WHOIS Lookup or WHOIS API. The products can be used to take indicators from your network, such as IP addresses, and query connected databases to retrieve relevant records and receive additional contextual information.

4. Thwarting IP Address Fraud

Fraudsters can go to great lengths to execute illegal schemes. One case, for instance, involved an IT firm that set up shell companies to fool a registry into allocating it 800,000 IP addresses. The company sold these to virtual private network (VPN) service providers, whose subscriber bases in need of anonymity comprised not just legitimate users but also hackers and cybercriminals.

Now say you come across the existence of similar fraudulent events and you want to alert the relevant entities, WHOIS Search or WHOIS API can help you retrieve the registration details of illegitimately obtained IP addresses. With an IP address's corresponding records at hand, you can identify the registry governing its use. The API also provides information as to when the IP address was released and last updated.

How to Use WHOIS API to Perform an IP Address WHOIS Lookup

WHOIS API is available for integration into a variety of security solutions and website plugins including Splunk and Wordpress. If you want to experience a free demo of the API, head over to the product's homepage, then type in an IP address into the field and hit the Enter key.

Below is an example output in XML format for the blacklisted IP address 201[.]18[.]18[.]173 (according to IP Blacklist Cloud, users reported the IP address for abuse over 1,000 times).

```
<WhoisRecord>
  <domainName>201.18.18.173</domainName>
  <parseCode>8</parseCode>
  <audit>
    <createdDate>2020-03-27 13:56:59.000 UTC</createdDate>
    <updatedDate>2020-03-27 13:56:59.000 UTC</updatedDate>
  </audit>
  <registrarName>LACNIC</registrarName>
  <registryData>
    <createdDate>20040831</createdDate>
    <updatedDate>20110610</updatedDate>
    <registrant>
      <name>Contato Administrativo Oi</name>
      <rawText>nic-hdl-br:  COAOI
person:       Contato Administrativo Oi
created:      20150723
changed:      20191212
nic-hdl-br:   COAOI
person:       Contato Administrativo Oi
created:      20150723
changed:      20191212</rawText>
    </registrant>
    <administrativeContact>
      <name>Centro de Gerencia de Rede TELEMAR</name>
      <rawText>nic-hdl-br:  CGR13
person:       Centro de Gerencia de Rede TELEMAR
created:      20000605
changed:      20170106
```

```
nic-hdl-br:  CGR13
person:      Centro de Gerencia de Rede TELEMAR
created:     20000605
changed:     20170106</rawText>
    </administrativeContact>
    <technicalContact>
      <name>Centro de Gerencia de Rede TELEMAR</name>
      <rawText>nic-hdl-br:  CGR13
person:      Centro de Gerencia de Rede TELEMAR
created:     20000605
changed:     20170106
nic-hdl-br:  CGR13
person:      Centro de Gerencia de Rede TELEMAR
created:     20000605
changed:     20170106</rawText>
    </technicalContact>
    <domainName>201.18.18.173</domainName>
    <rawText>% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% Brazilian resource: whois.registro.br
```


The report shows that the Latin America and Caribbean Network Information Centre (LACNIC) is the regional internet registry behind the IP address. It also reveals the registrant's name "Oi" to whom the IP address has been allocated. Oi is a major telco company and internet service provider (ISP) in Brazil and Latin America. Analysts and law enforcement agents can reach out to it to retrieve any additional information about the IP address for further investigation.

IP address WHOIS lookups can be part of robust processes in threat hunting, incident response, and cyber investigation. Indeed, WHOIS Lookup and WHOIS API enable infosec professionals and law enforcement agents to track the identities of criminals with as much as an IP address.