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, helpfully routing users to the correct hosts or websites. However, because of inherent DNS design flaws, attackers can spoof IP addresses. In fact, they may do so to misdirect users to dangerous sites. Therefore, it is critical to routinely scan the IP addresses passing through your network filters to ensure their integrity and identify if any has potential links to malicious campaigns or networks.

Part of this process is retrieving the WHOIS records of an IP address, which is doable via WHOIS Lookup or WHOIS API to extract their ownership details for further inspection. Both products provide additional valuable details, including the domains hosted on an IP address and which regional Internet registry (RIR) manages the resource.

Why Run an IP WHOIS Lookup?

Let's take a closer look at some specific areas where a WHOIS IP address search can be helpful.

1. Payment Fraud Investigation

Authorities can stay hot on the trail of cybercriminals by tracking the origin of their IP addresses. Fraudsters paying for purchases using stolen payment cards are also identifiable based on the IP addresses logged when they made orders.

Investigators can check the suspicious IP addresses from the merchant's and payment processor's interfaces. Then, they can run the IP addresses on WHOIS Lookup or WHOIS API to obtain their owners' names and contact details and connected domains, if any.

2. DNS Forensic Analysis

A WHOIS IP address lookup can enhance the data gathered from open-source intelligence (OSINT) sources to more comprehensively analyze IP addresses attempting to establish connections with an organization's systems.

In the wake of a malware attack, for example, you can use OSINT sources to determine if your network is communicating with known command-and-control (C&C) servers by screening the IP addresses recorded in your logs. If you find suspicious IP addresses, you can analyze their WHOIS records to see if they share patterns with known cybercriminal networks.

3. Threat Intelligence Gathering

IP WHOIS records can enrich threat intelligence sources with the up-to-date ownership and administrative details of suspicious and malicious resources. For instance, security solutions providers can use WHOIS API to update their blocklists with reliable WHOIS data automatically.

Adding accurate WHOIS context to malicious IP addresses can help map out their digital infrastructure. Security analysts and investigators can then use these enriched sources for threat hunting and predictive threat intelligence gathering.

4. Thwarting IP Address Fraud

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

Now, say you come across similar fraudulent events, and you want to alert the relevant entities. WHOIS Lookup or WHOIS API can help you retrieve the registration details of illegitimately obtained IP addresses. You can identify the registries governing their use with each IP address's corresponding records. The tools also provide information on when an IP address was released and last updated.

How to Use WHOIS API to Perform an IP WHOIS Lookup

WHOIS API is available for integration into various security solutions and website plug-ins, including Splunk and WordPress. If you want to see a free API demo, head over to the product's home page

, then type an IP address into the field and hit the Enter key.

Below is a sample output in XML format for the malicious IP address 65[.]49[.]1[.]52. According to AbuseIPDB, users reported the IP address for abuse more than 1,600 times in a span of two months.


```
<WhoisRecord>
  <domainName>65.49.1.52</domainName>
  <rawText>%rwhois V-1.5:0012b7:00 concierge.he.net (HE-RWHOISd v:b9ccd6e)
network:ID;I:NET-65.49.1.0/24
network:Auth-Area:nets
network:Class-Name:network
network:Network-Name;I:NET-65.49.1.0/24
network:Parent;I:NET-65.49.0.0/17
network:IP-Network:65.49.1.0/24
network:Org-Contact;I:POC-CE-2897
network:Tech-Contact;I:POC-HE-NOC
network:Abuse-Contact;I:POC-HE-ABUSE
network:NOC-Contact;I:POC-HE-NOC
network:Created:20230602163031000
network:Updated:20230602163031000

contact:ID;I:POC-CE-2897
contact:Auth-Area:contacts
contact:Class-Name:contact
contact:Name:R[redacted] P[redacted]
contact:Company:The Shadow Server Foundation
contact:Street-Address:4695 Chabot Dr. Suite 200
contact:City:Pleasanton
contact:Province:CA
contact:Postal-Code:94588
contact:Country-Code:US
```

```
contact:Auth-Area:contacts
contact:Class-Name:contact
contact:Name:Network Operations Center
contact:Company:Hurricane Electric
contact:Street-Address:760 Mission Ct
contact:City:Fremont
contact:Province:CA
contact:Postal-Code:94539
contact:Country-Code:US
contact:Phone:+1-510-580-4100
contact:E-Mail:noc@he.net
contact:Created:20100901200738000
contact:Updated:20100901200738000

contact:ID;I:POC-HE-ABUSE
contact:Auth-Area:contacts
contact:Class-Name:contact
contact:Name:Abuse Department
contact:Company:Hurricane Electric
contact:Street-Address:760 Mission Ct
contact:City:Fremont
contact:Province:CA
contact:Postal-Code:94539
contact:Country-Code:US
contact:Phone:+1-510-580-4100
contact:E-Mail:abuse@he.net
```

```
network:ID;I:NET-65.49.1.0/24
network:Auth-Area:nets
network:Class-Name:network
network:Network-Name;I:NET-65.49.1.0/24
network:Parent;I:NET-65.49.0.0/17
network:IP-Network:65.49.1.0/24
network:Org-Contact;I:POC-CE-2897
network:Tech-Contact;I:POC-HE-NOC
network:Abuse-Contact;I:POC-HE-ABUSE
network:NOC-Contact;I:POC-HE-NOC
network:Created:20230602163031000
network:Updated:20230602163031000
contact:ID;I:POC-CE-2897
contact:Auth-Area:contacts
contact:Class-Name:contact
contact:Name:R[redacted] P[redacted]
contact:Company:The Shadow Server Foundation
contact:Street-Address:4695 Chabot Dr. Suite 200
contact:City:Pleasanton
contact:Province:CA
contact:Postal-Code:94588
contact:Country-Code:US
contact:Phone:-
contact:E-Mail:-
contact:Created:20180817203001000
contact:Updated:20220114163002000
```

Breaking down the IP WHOIS report of the malicious resource, we can extract pertinent information, including:

- **Registrant organization:** Hurricane Electric LLC

- **Country:** U.S.
- **Creation date:** October 4, 2007
- **Last update date:** February 24, 2012
- **ISP:** The Shadow Server Foundation
- **Network contact name:** R***** P*****
- **Registry:** ARIN

The IP WHOIS report also includes the contact details of the ISP and registrant, including their phone numbers and email addresses.

Alternatively, users can utilize WHOIS Lookup for free to perform a similar research. The tool provides all the registration information for an IP address in seconds.

—

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

Test our WHOIS lookup tools firsthand, or contact us for more information about how our IP and domain intelligence sources can enrich your processes.