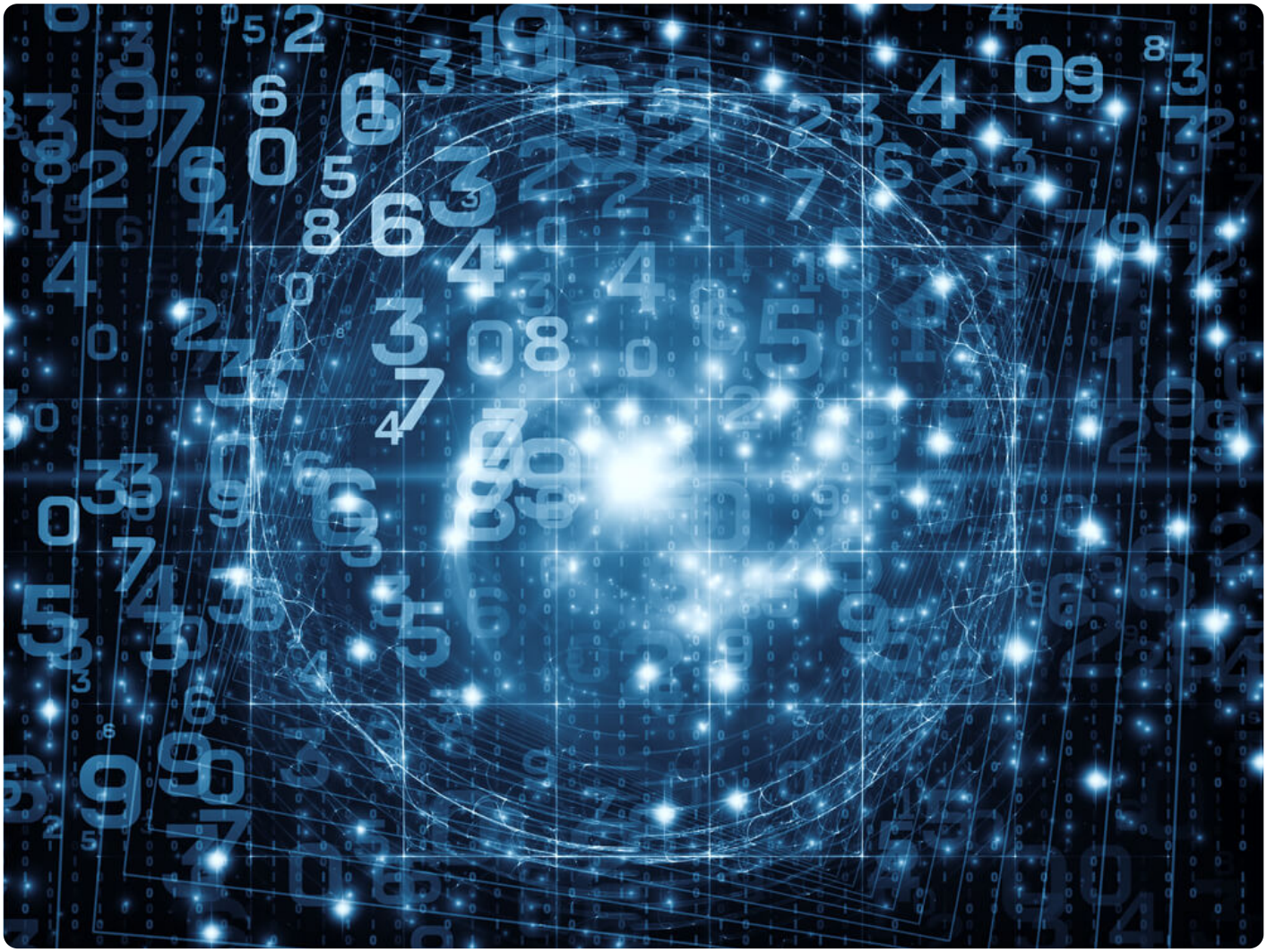
What You Can Find Out from a WHOIS IP Search

Posted on June 15, 2020



Did you know that an IP address can be a good starting point for a cybercrime investigation or even just a routine check of suspicious activities? For instance, when you go to malware data feeds, or any threat intelligence site, one of the usual indicators of compromise (IoCs) you'll see are known malicious IP addresses.

However, like any threat data, an IP address becomes utterly useless when it doesn't provide any meaningful details. What then? Tools such as WHOIS Lookup might help to dig deeper.

So, what exactly is WHOIS Lookup, and what information can it provide about an IP address?

What Is a WHOIS Lookup?

WHOIS Lookup is a web-based tool that enables you to perform a WHOIS IP search. With it, you can get hold of key data points about an IP address, a domain name, or an email address. And so if a cybersecurity team can obtain even one of those three details, it can already serve as a good starting point.

In particular, WHOIS Lookup has access to a regularly updated database that contains more than 7 billion WHOIS records. And since it is web-based, you don't need to download and set up anything on your computer. You can run queries on the fly.

But if you plan to do a massive WHOIS IP search, you could use Bulk WHOIS Lookup, where you can upload a comma-separated values (CSV) or text file that contains a list of domain names, IP addresses, or email addresses that you want to investigate.

Investigative Questions About an IP Address That WHOIS Lookup Can Answer

Whether you're doing one WHOIS IP search at a time or using the bulk WHOIS service, you can obtain answers to several questions. We used 154[.]211[.]102[.]50, the IP address of the domain rtsg[.]consider7[.]cn listed as an attack IoC on PhishTank. (We obtained the IP address by running

the malicious domain on DNS Lookup API.) Here's what we found out:

1. Who is the IP address's registrar?

The WHOIS IP search would return the name of the registrar, which is usually the regional Internet registry (RIR) for the user's region. It could thus be the African Network Information Centre (AFRINIC), the American Registry for Internet Numbers (ARIN), the Asia-Pacific Network Information Centre (APNIC), the Latin America and Caribbean Network Information Centre (LACNIC), or the Réseaux IP Européens Network Coordination Centre (RIPE NCC).

More importantly, you would also see the email address you can contact in case of abuse. The email address usually belongs to the user's Internet service provider (ISP).

The IoC we are investigating is under the jurisdiction of AFRINIC, while the abuse contact email address was tech@cloudinnovation[.]org (in case you wish to report the IP address).

2. Who is the IP address's registrant?

In some cases where cybercriminals use dynamic IP addresses, you won't be able to see the name and address of the registrant. But the tool would return the country and use type (i.e., residential or commercial).

In this particular case, the tool returned the registrant details of the IP address we are looking into. It tells us that the IP address belongs to CloudInnovation Infrastructure, an organization based in Hong Kong.

```
<WhoisRecord>
  <domainName>154.211.102.50</domainName>
  <parseCode>8</parseCode>
  <audit>
    <createdDate>2020-03-06 11:22:47.000 UTC</createdDate>
    <updatedDate>2020-03-06 11:22:47.000 UTC</updatedDate>
  </audit>
  <registrarName>AFRINIC</registrarName>
  <registrarIANAID>778</registrarIANAID>
  <registryData>
    <updatedDate>tech@cloudinnovation.org 20160215</updatedDate>
    <registrant>
      <name>CloudInnovation infrastructure</name>
      <organization>CloudInnovation</organization>
      <country>HONG KONG</country>
      <countryCode>HK</countryCode>
      <rawText>netname:        CloudInnovation
descr:          CloudInnovation infrastructure
country:        HK
</rawText>
    </registrant>
    <domainName>154.211.102.50</domainName>
    <status>ASSIGNED PA</status>
    <rawText>% This is the AfriNIC Whois server.
```


3. What are the registrant's contact details?

For our IoC, WHOIS Lookup revealed an interesting detail. While CloudInnovation is Hong Kong-based, its designated contact Cloud Innovation Support has an address from the Seychelles.

```
person:         Cloud Innovation Support
address:        Ebene
address:        MU
address:        Mahe
address:        Seychelles
phone:          tel:+248-4-610-795
e-mail:         tech@cloudinnovation.org
nic-hdl:        CIS1-AFRINIC
abuse-mailbox:  abuse@cloudinnovation.org
mnt-by:         CIL1-MNT
changed:        tech@cloudinnovation.org 20160215
source:         AFRINIC</rawText>
    <parseCode>1080</parseCode>
    <header>% This is the AfriNIC Whois server.
% This is the AfriNIC Whois server.</header>
    <strippedText>
% Information related to '154.211.102.0 - 154.211.102.255'
```

4. What is the IP address's NetRange and NetName?

Other important details that a WHOIS IP search provides for cybersecurity experts include the IP address's NetRange and NetName. In this case, the IP address range associated with thephishing IoC is 154[.]211[.]102[.]0–154[.]211[.]102[.]255, while the net name is CloudInnovation.That tells us that the registrant owns a block of IP addresses.

5. Is the IP address currently in use?

WHOIS Lookup also reveals the status of the IP address, which in this case, is "Assigned PA." That means that a local Internet registry assigned the IP address to one of its customers.

Overall, all of the details obtained from WHOIS Lookup about the IoC may be enough for investigators to dig deeper. For instance, the IP address can be run through a reverse IP/DNS lookup tool to see if other domains resolve to it. Some of them may also be malicious.

Doing a WHOIS IP search using WHOIS Lookup is an effective way to gather as much information as possible about a given IP address. That sort of intelligence helps cybersecurity professionals beef up their overall network security when used alongside security systems such as threat intelligence platforms and security information and event management (SIEM) software.