How to Find My or Someone Else's IP Range with IP Netblocks WHOIS Database and IP Netblocks API

Posted on June 24, 2020

Hackers are known to hijack IP addresses for use in various illegal activities. They could thus use your IP address in a malicious campaign, but that doesn't mean you're guilty. And so, your infosec team needs to gather enough evidence to counter accusations of foul play against you. You may also need to help the authorities by looking into who is behind a threat.

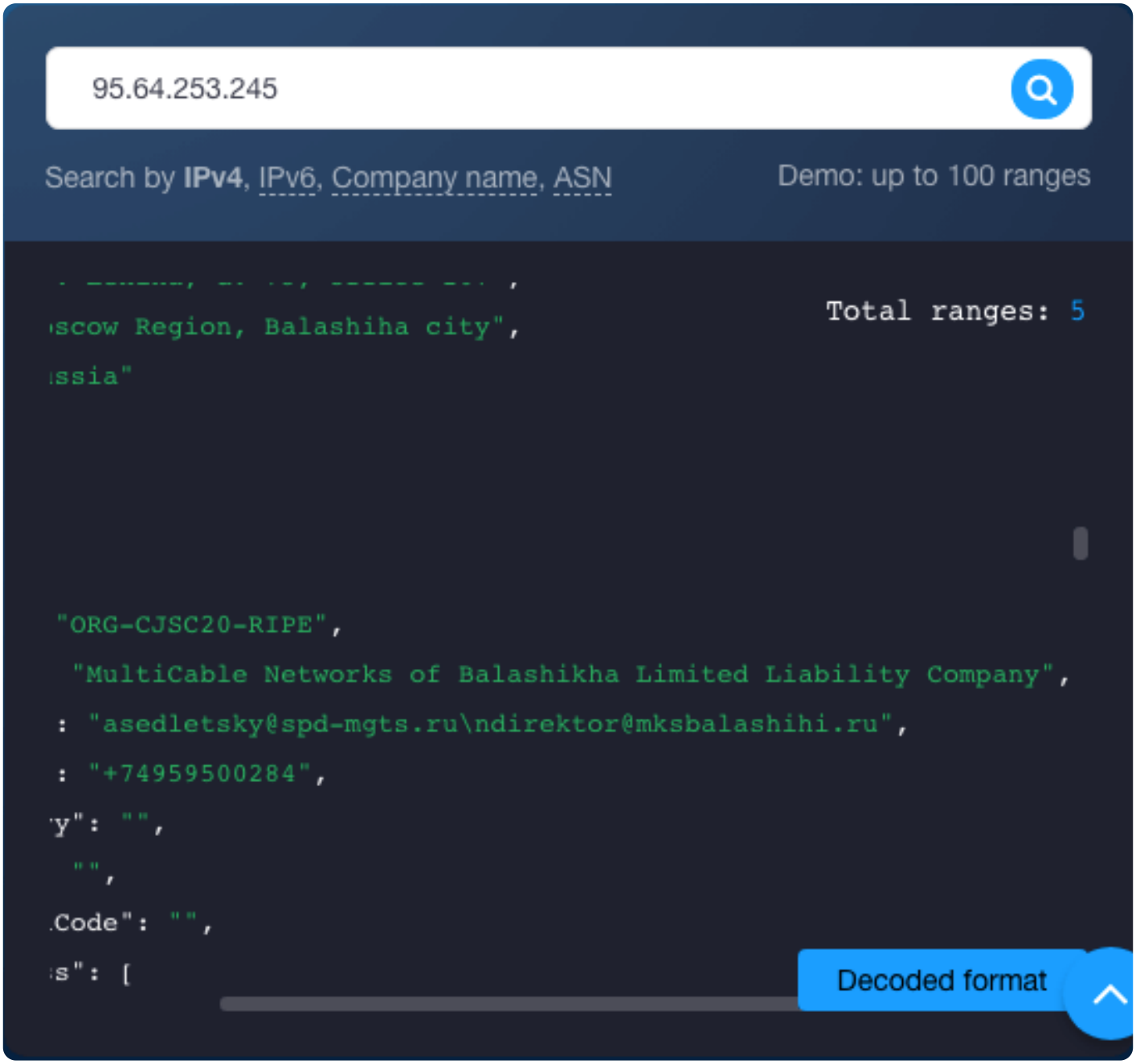
The first step in that direction is answering the question: What is my IP range? Solutions like IP Netblocks API or IP Netblocks WHOIS Database could be of help. That's not where the buck stops, though, you'll need to use a host of IP and domain intelligence tools next. For this reason, we created this guide for you.

Guide to Identifying the Real Threat Actor Starting with IP Netblocks API or IP Netblocks WHOIS Database

Let's say, for example, that a company accused your organization of foul play as the IP address 95[.]64[.]253[.]245 that has been trying to access one of their restricted systems repeatedly points to you. What do you do?

1. Gather Details about Your IP range using IP Netblocks API/IP Netblocks WHOIS Database

IP Netblocks API and IP Netblocks WHOIS Database provide detailed ownership information about an IP range.



You found that the IP address in question is indeed included in five ranges. The narrowest two of these ranges can be explicitly linked to the Internet service provider (ISP) MultiCable Networks of Balashikha Limited Liability Company. Indeed, the first range, 95[.]64[.]128[.]0 to 95[.]64[.]255[.]255, and the second (broader) range, 95[.]64[.]128[.]0 to 95[.]64[.]255[.]255, have

been allocated to the ISP. In both cases, the company has appointed m.kuschuk@mksbalashihi[.]ru as a contact point.

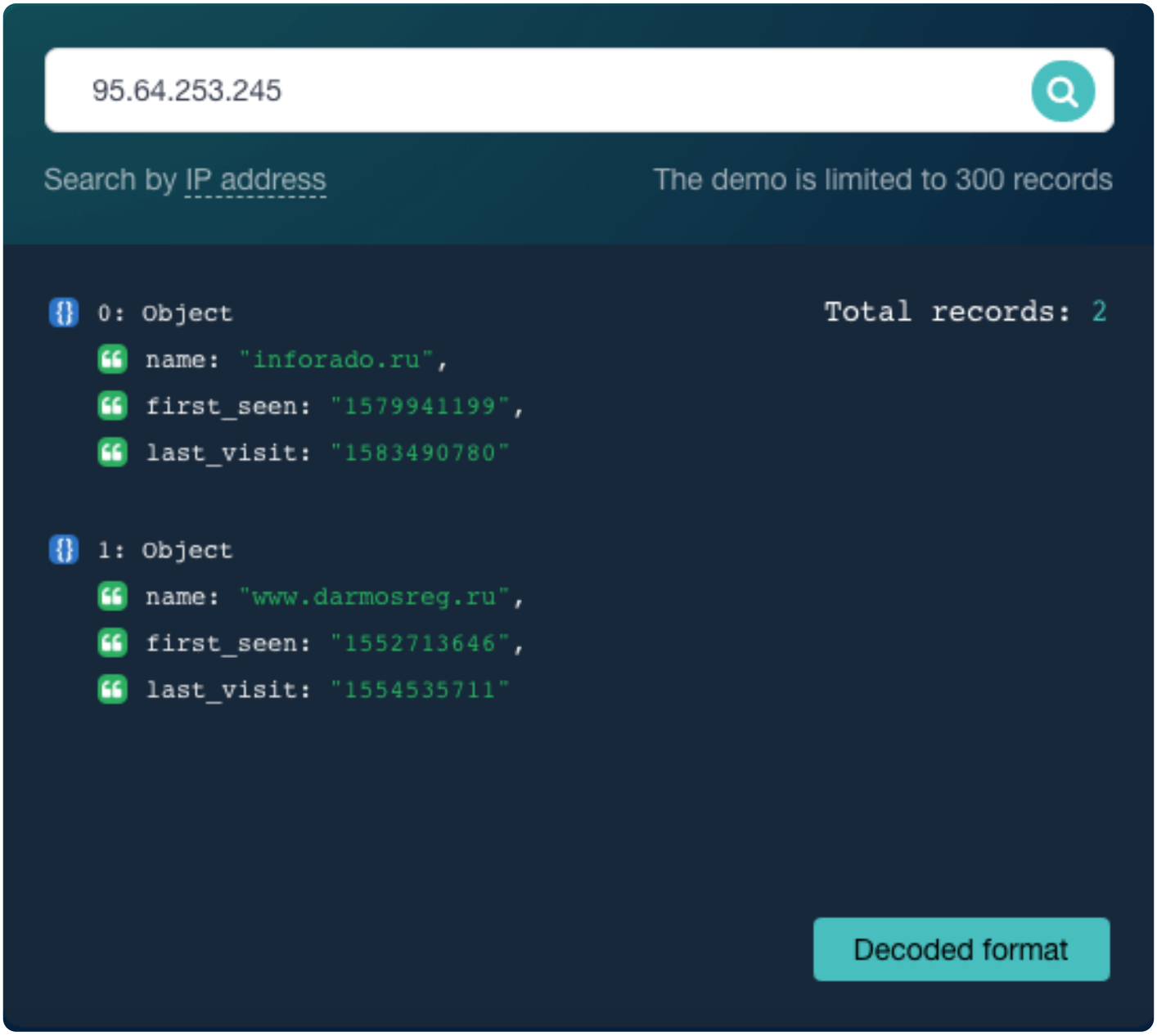
The query results also show that all the ranges are under the jurisdiction of the Reseaux IP Europeens Network Coordination Centre (RIPE NCC), and reports of abuse can be sent to abuse@ripe[.]net or hostmaster@ripe[.]net.

Downloading IP Netblocks WHOIS Database and looking up the information would give you the same results.

2. Use Reverse IP/DNS API to look for connected domains

In this scenario, you are aware that you are using a shared IP address. So, if not you, one of the domains hosted on your IP address may thus be at fault. Reverse IP/DNS API can help you obtain a list of all the domains you share the IP address with.

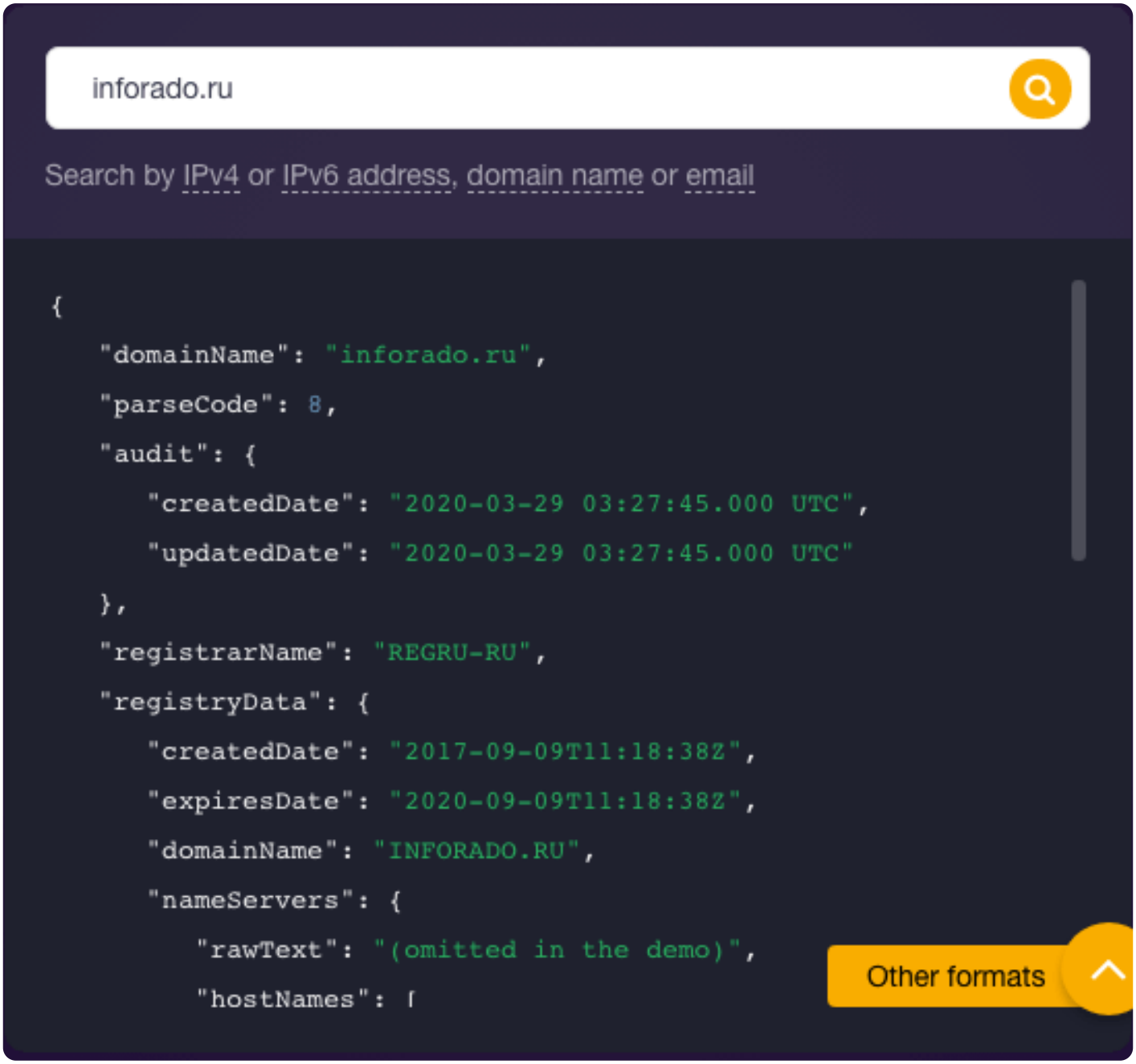
The inputting of your IP address into the tool gives you two domains hosted on 95[.]64[.]253[.]245.

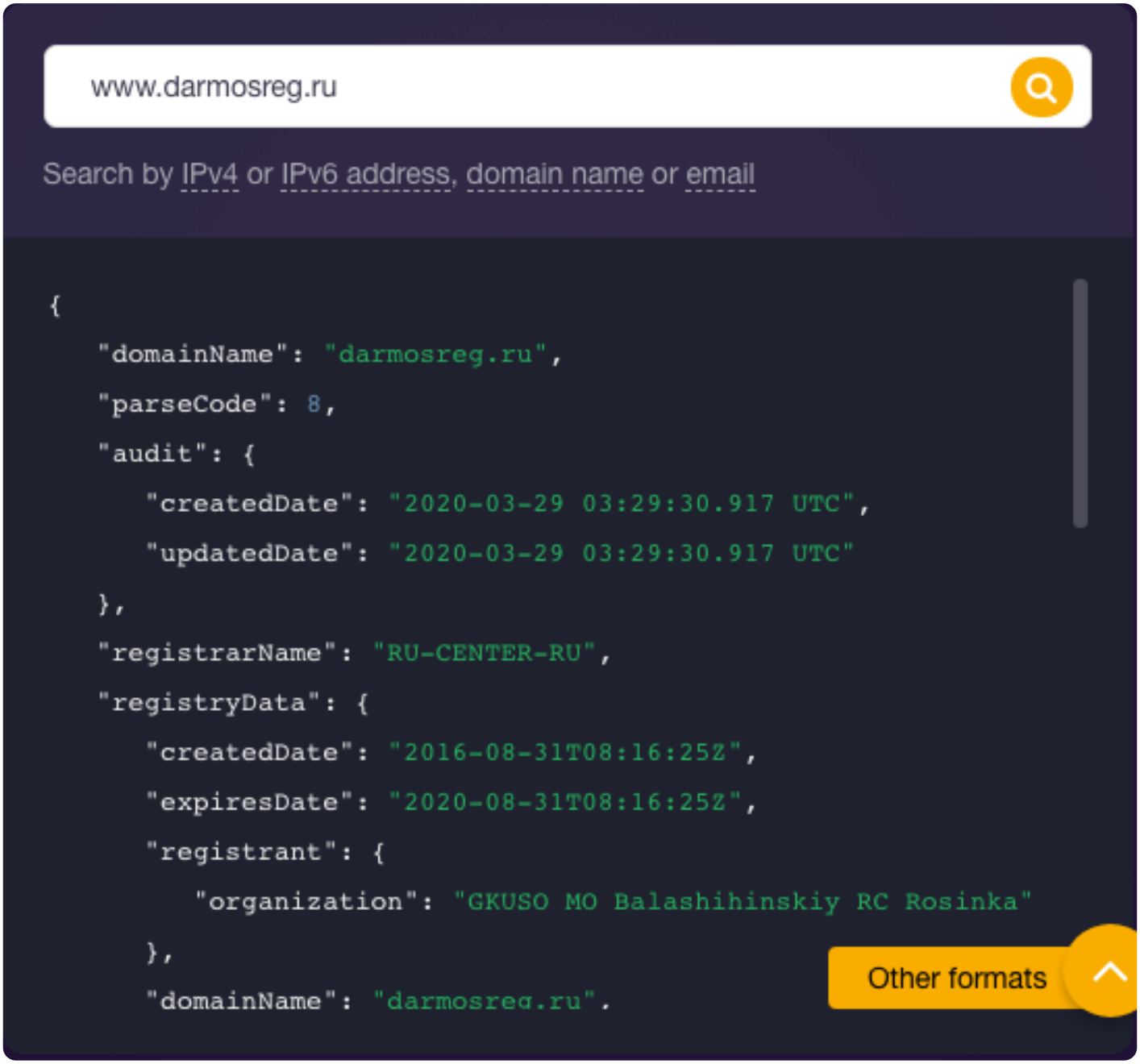


For the sake of the example, let's say that your domain is www[.]darmosreg[.]ru in this hypothetical scenario. The other domain inforado[.]ru, on the other hand, doesn't belong to you.

3. Get the domains’ ownership details with WHOIS API

You’ll need proof that you don’t own the other domain for your case. You can rely on WHOIS API for that to give you the following details:


inforado.ru
Search by IPv4 or IPv6 address, domain name or email
{
"domainName": "inforado.ru",
"parseCode": 8,
"audit": {
"createdDate": "2020-03-29 03:27:45.000 UTC",
"updatedDate": "2020-03-29 03:27:45.000 UTC"
},
"registrarName": "REGRU-RU",
"registryData": {
"createdDate": "2017-09-09T11:18:38Z",
"expiresDate": "2020-09-09T11:18:38Z",
"domainName": "INFORADO.RU",
"nameServers": {
"rawText": "(omitted in the demo)",
"hostNames": [
Other formats


www.darmosreg.ru
Search by IPv4 or IPv6 address, domain name or email
{
"domainName": "darmosreg.ru",
"parseCode": 8,
"audit": {
"createdDate": "2020-03-29 03:29:30.917 UTC",
"updatedDate": "2020-03-29 03:29:30.917 UTC"
},
"registrarName": "RU-CENTER-RU",
"registryData": {
"createdDate": "2016-08-31T08:16:25Z",
"expiresDate": "2020-08-31T08:16:25Z",
"registrant": {
"organization": "GKUSO MO Balashihinskiy RC Rosinka"
},
"domainName": "darmosreg.ru",
Other formats

Interestingly, your domain darmosreg[.]ru isn't privacy-protected. It shows your company as its registrant, which is proof that you are not hiding anything. The registrant of the other domain inforado[.]ru doesn't appear on its WHOIS record (i.e., there is no field "registrant" as in the case of the other domain).

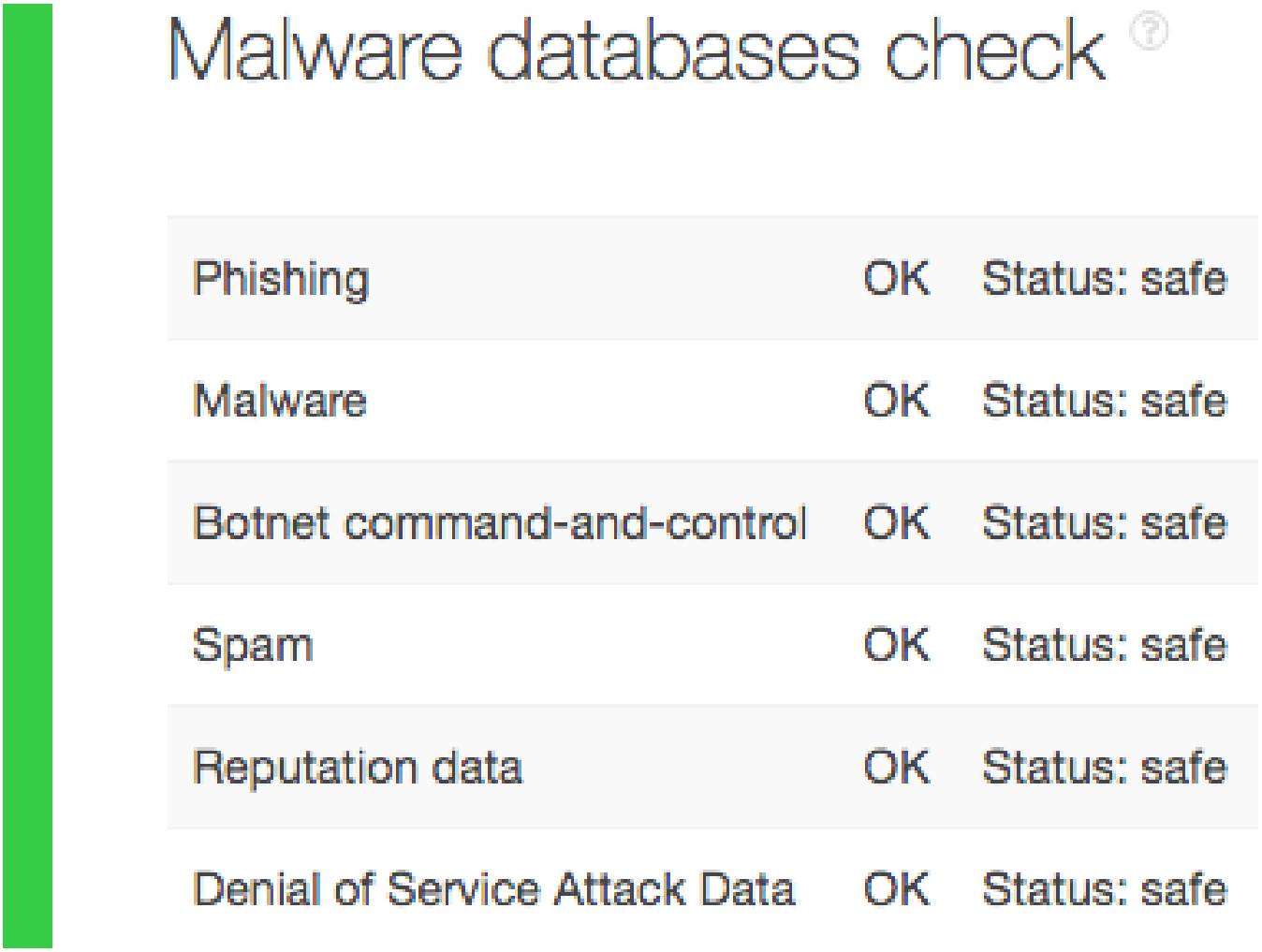
4. Check your and other domains on the same IP address for ties to malicious activity using Threat Intelligence Platform

Since a company is accusing you of malicious activity, you need to prove that your domain is clean. You can use the Threat Intelligence Platform (TIP) among other solutions for that.

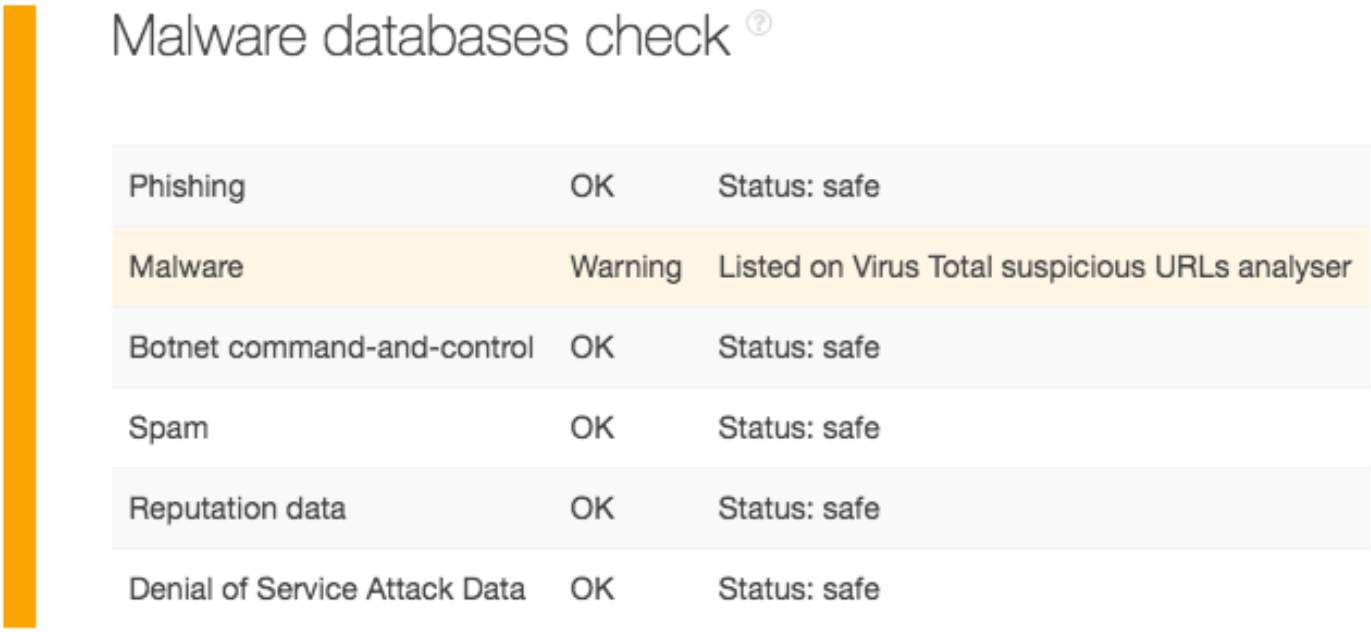
A query for your domain name darmosreg[.]ru on TIP reveals that it is threat-free for the following aspects:

Potentially dangerous content

Links to .apk files	OK
Links to .exe files	OK
Iframes	OK
Scripts opening new windows	OK
Redirects	OK



Our query for the domain inforado[.]ru, meanwhile, shows that it appears on VirusTotal's suspicious URLs database. It is, therefore, malicious. It may also be the one responsible for a particular malicious activity.



5. Pool all your evidence and send it to your accuser and the authorities

Now that you have all the data you need, you can contact your accuser and tell the organization that you just happen to share an IP address with a malicious domain that has no actual ties to your company. You can submit all of your findings to your ISP as well, along with the accusation against your business. What's more, you can ask your ISP to assign you a different IP address so you'd no longer have to deal with similar allegations in the future.

By now, you've probably realized how vital knowing and keeping your IP and its IP range threat-free is to avoid severe repercussions such as being accused of launching attacks. IP range lookups via IP Netblocks API or IP Netblocks WHOIS Database are a crucial first step in performing in-depth investigations concerning IP addresses.