IP Netblocks API to Fight Cybercrime: Performing an IP Range Lookup & Other Steps

Posted on May 26, 2020

It is pretty standard for cybercriminals to spend time exploring a network for weaknesses they can exploit. That's why cybersecurity experts must continuously monitor their systems and logs for any signs of future attacks. They can do so with various IP and domain intelligence tools, notably using IP Netblocks API as a first step.

How exactly? In this post, we provide a demonstration of how organizations can better ensure their infrastructure's security and possibly even prevent breaches.

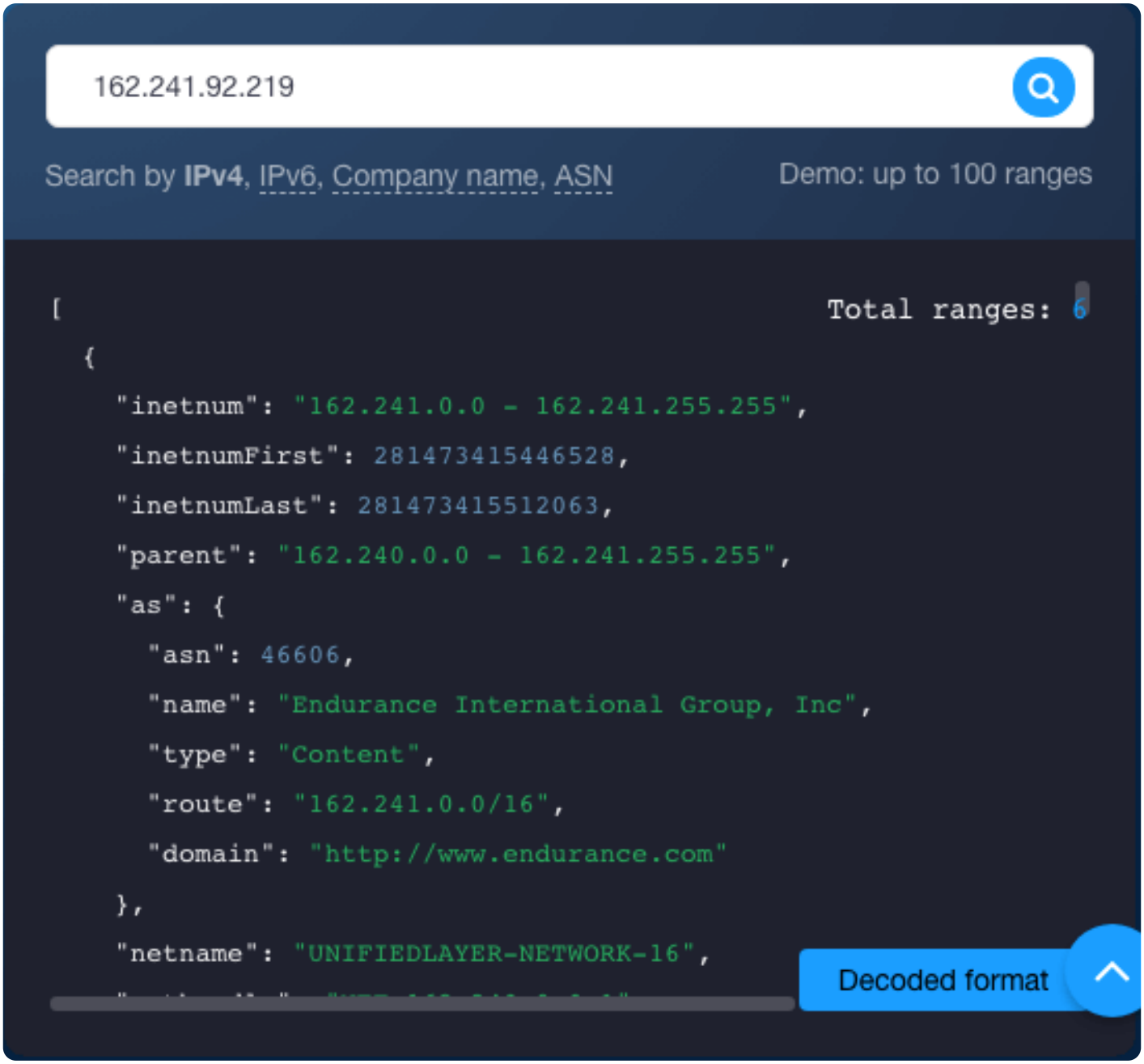
A Step-by-Step Guide Beginning with the Use of IP Netblocks API for Cyberdefense

Imagine that your security IT team discovered that the IP address 162[.]241[.]92[.]219 has been attempting to access a restricted or confidential system in your corporate network. You can follow this step-by-step guide to uncovering a potentially damaging threat with IP Netblocks API at the forefront.

1. Use IP Netblocks API to uncover the offending IP address's host

A persistent attempt to access a confidential file may require immediate action. That means reporting the issue to the IP address's owner, host or issuer (i.e., Internet service provider [ISP]), or regional Internet registry (RIR) in that particular order. Finding out who these entities are is easy with IP Netblocks API.

Our query for 162[.]241[.]92[.]219 revealed that the IP address is part of the range 162[.]241[.]0[.]0–162[.]241[.]255[.]25. It's owned by IT service provider Endurance International Group, Inc. Additionally, the IP address in question has ties to the domain https[:]//www[.]endurance[.]com/, the service provider's website.

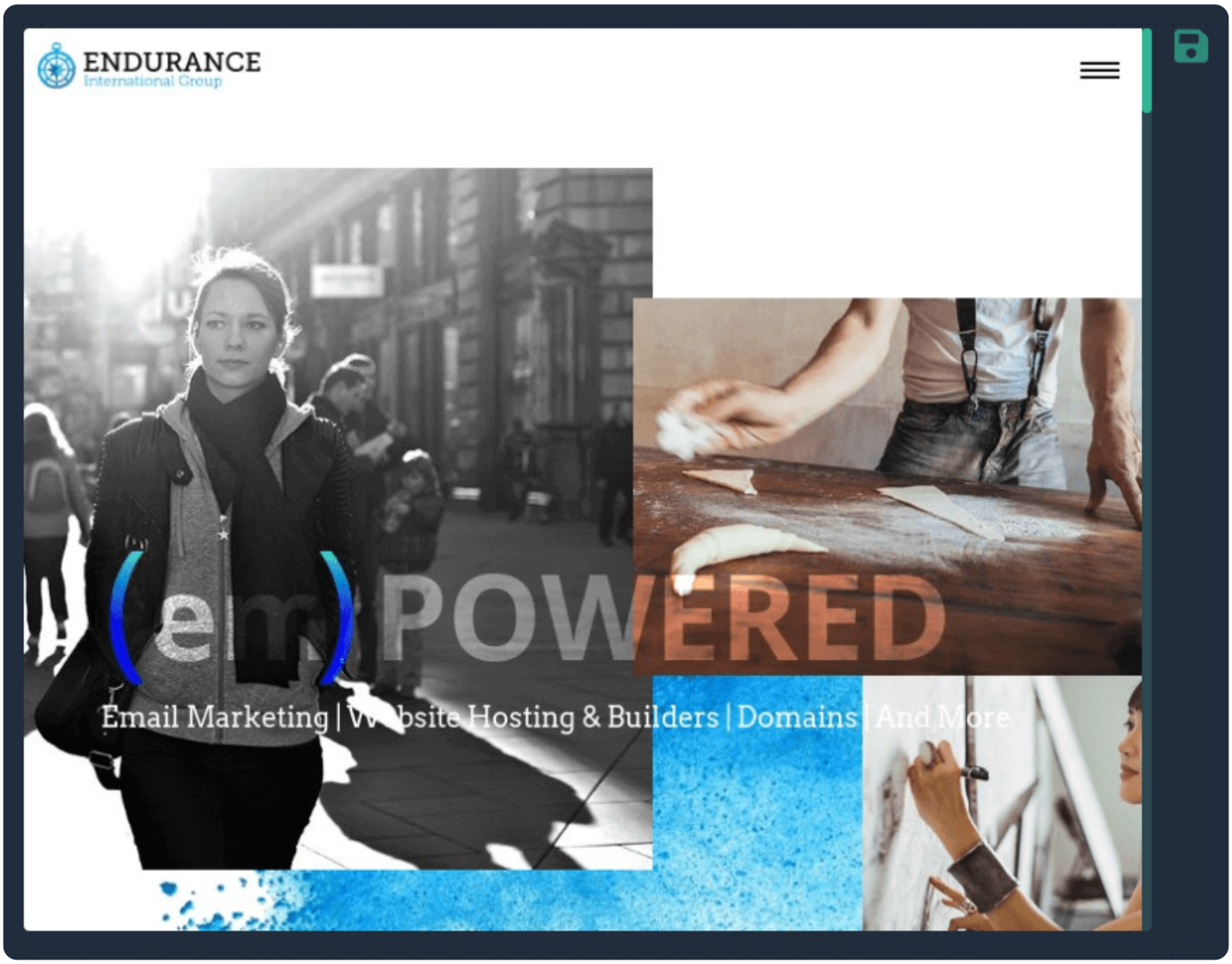


What's more, we found that Bluehost is the hosting provider, and the address falls under the jurisdiction of the American Registry for Internet Numbers (ARIN). We also retrieved three abuse contact email addresses from the IP Netblocks API query—abuse@bluehost[.]com, neig-net-team@endurance[.]com, and neig-noc@endurance[.]com.

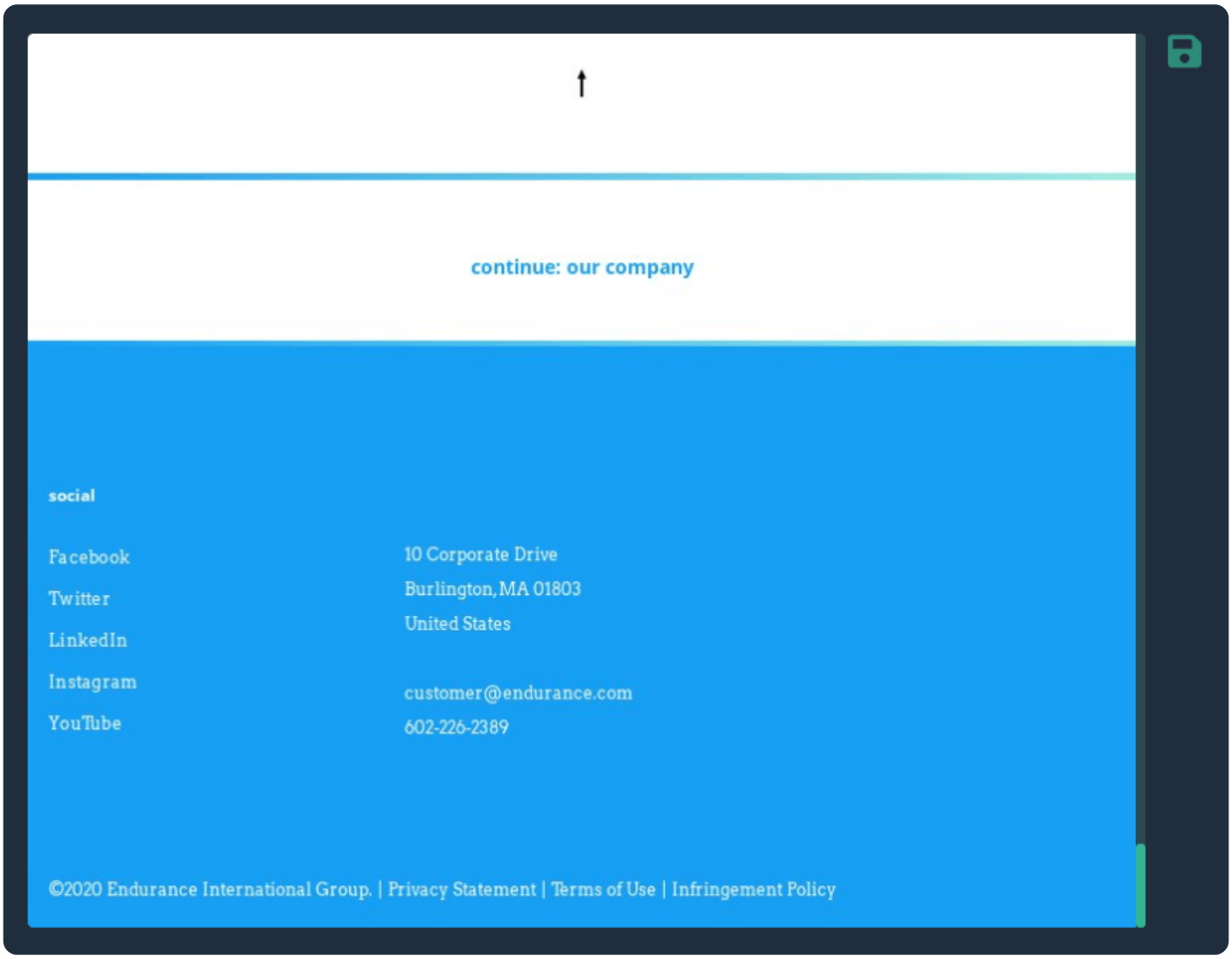
The affected user can contact these email addresses first to report the issue. Note that it is vital to gather as much information as possible before turning to higher authorities (i.e., ISPs and RIRs).

2. Access the investigated domain without bothering with Screenshot API

While unwary users may not mind directly accessing potentially dangerous domains on their browsers, the more security-savvy ones would think twice before doing so. The main reason for this is that they may unnecessarily visit a compromised site and thus get their systems infected with malware. To avoid such a complication, users can rely on Screenshot API. Our query of https[:]//www[.]endurance[.]com/ returned this result:



Another screenshot also gave out other contact details that may be useful in getting to the bottom of the issue. It may be worth a try contacting the service provider through the available channels, too.

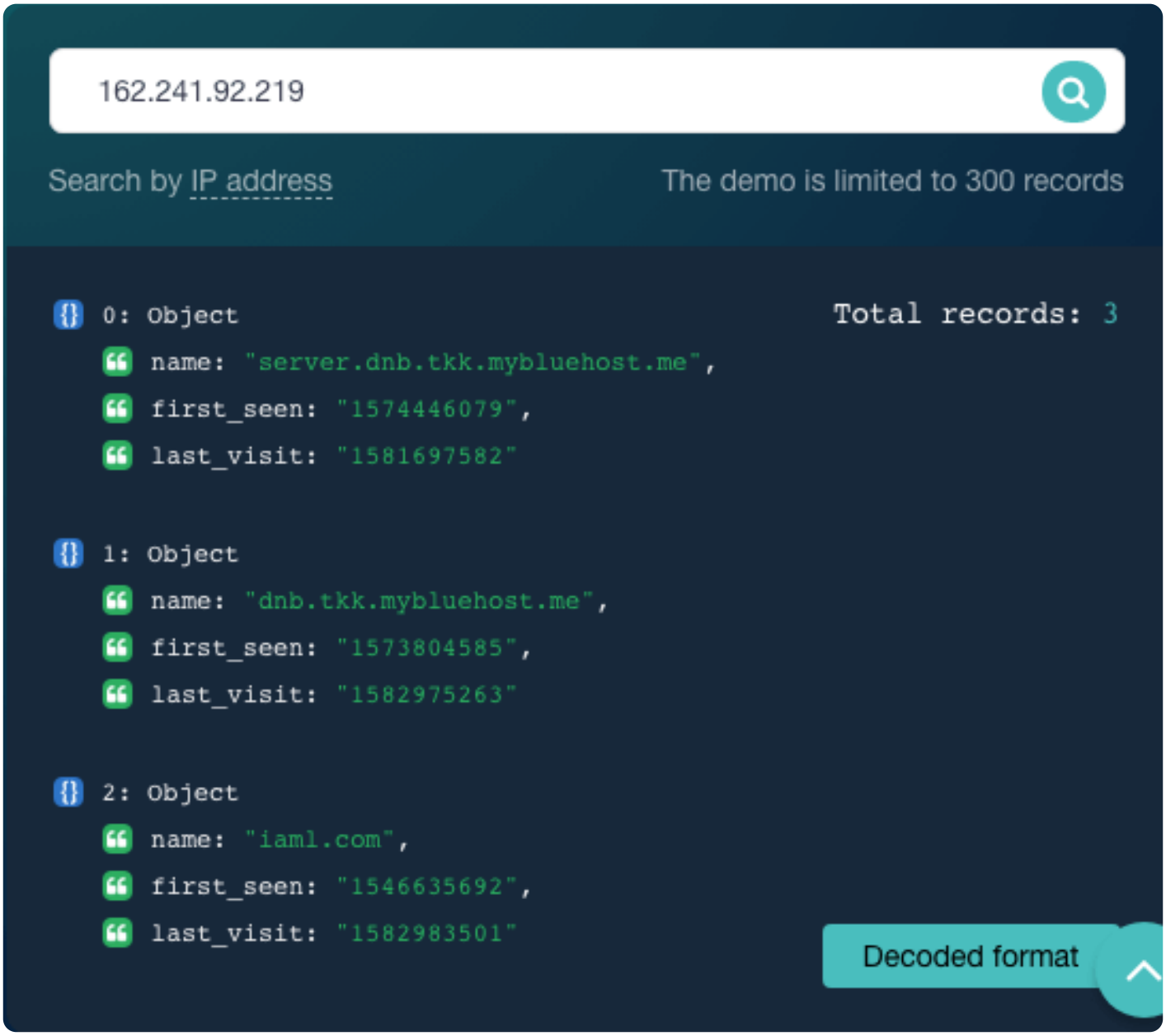


But while our investigation so far brought us to this website, the page seems pretty legitimate, so we decided to keep looking in other directions as part of the next step.

3. Use Reverse IP/DNS API to identify connected domains

It is common practice for ISPs to issue shared IP addresses to users. This particular scenariocould be one of those cases. To ensure that you are not accusing the wrong entity, you need toidentify all of the domains hosted on the IP address in question.

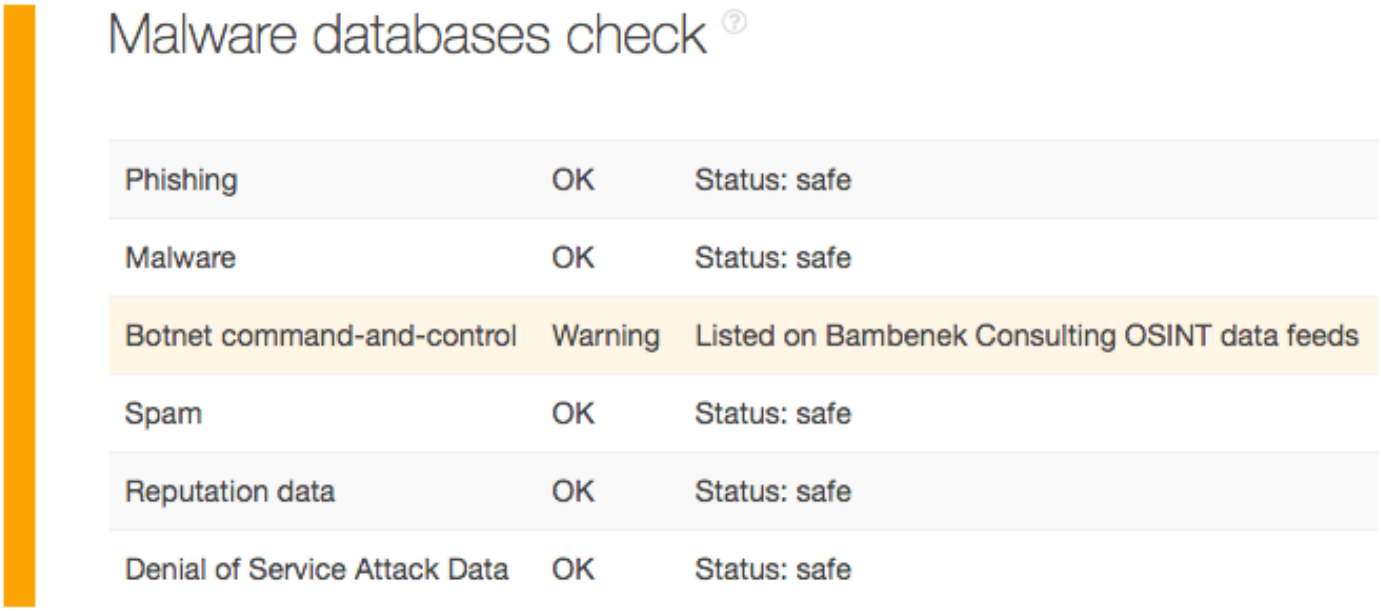
Reverse IP/DNS API can help with that. Our query for 162[.]241[.]92[.]219 returned three domains hosted on it—server[.]dnb[.]tkk[.]mybluehost[.]me, dnb[.]tkk[.]mybluehost[.]me, and iaml[.]com.



That tells us that the IP address is indeed a shared one and is, like the IP Netblocks API data showed, under Bluehost's management.

4. Use Threat Intelligence Platform to check if the connected domains have ties to malicious activities

The additional information now lets us dig deeper into the domains via Threat Intelligence Platform (TIP). Our queries revealed that iaml[.]com might be the real threat source as it appears on the Bambenek Consulting OSINT Data Feeds as a botnet command-and-control (C&C) server. That gives us sufficient evidence to consider blocking the domain from one's network. This step might also alleviate unwanted access to the restricted file.



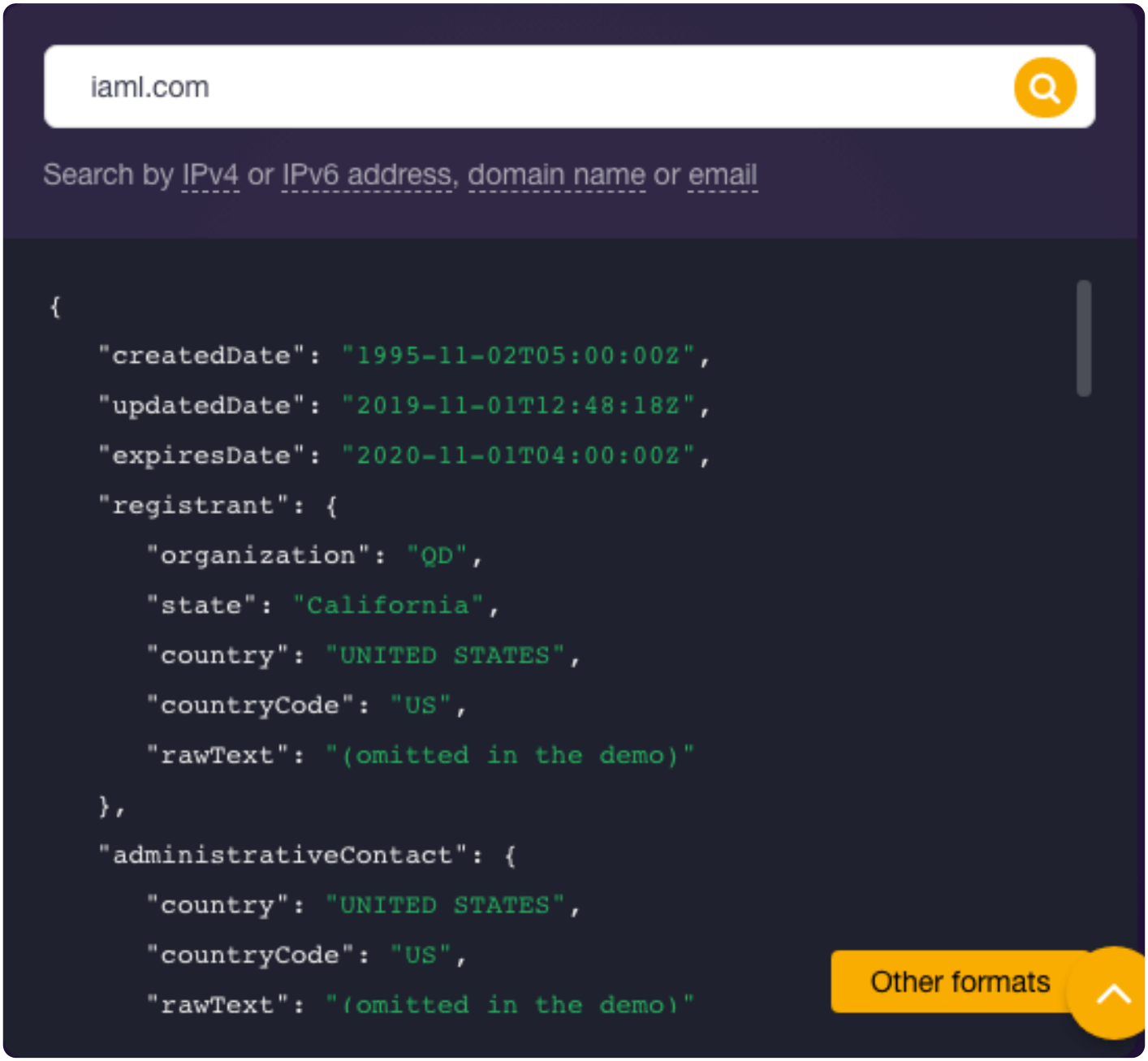
Malware databases check

Phishing	OK	Status: safe
Malware	OK	Status: safe
Botnet command-and-control	Warning	Listed on Bambenek Consulting OSINT data feeds
Spam	OK	Status: safe
Reputation data	OK	Status: safe
Denial of Service Attack Data	OK	Status: safe

The other two domains dnb[.]tkk[.]mybluehost[.]me and server[.]dnb[.]tkk[.]mybluehost[.]me where Endurance International Group's website may have connections to (hint: they're likely Bluehost-owned) are probably safe to access.

5. Identify the offending domain’s owner with WHOIS APIs

Now that we have identified a plausibly dangerous domain (and possibly the root of the issue in our scenario)—iaml[.]com, we need to identify its owner. We used WHOIS API for that and found that the domain belongs to a U.S.-based organization called “QD.”



Unfortunately, the current WHOIS record didn't give out any contact details. But the affected user can file a complaint with the registrar—GoDaddy. Moreover, digging into the domain's history with WHOIS History API would show that it pertained to a certain "Michael Mills" at least up until July 2017. So, while it seems there has been a change of owner, his name might be worth a mention

when following up with the relevant entities.

6. Finalize the report so concerned entities can take action

Once you pool all of the data gathered, you can now contact the authorities and give them the evidence gathered so they can further investigate and take the actions they consider necessary.

As you've seen, investigations that begin with a simple IP range lookup can indeed lead to a much deeper cybersecurity search. IP Netblocks API can provide cybersecurity professionals with a starting point from which to pivot an in-depth investigation. Data from the API augments threat intelligence obtained from network logs and external reports so investigators can follow up from there and get to the bottom of an issue.