Afeefah Manzoor

ITN 295: Gateways to the Dark Web

Steps:

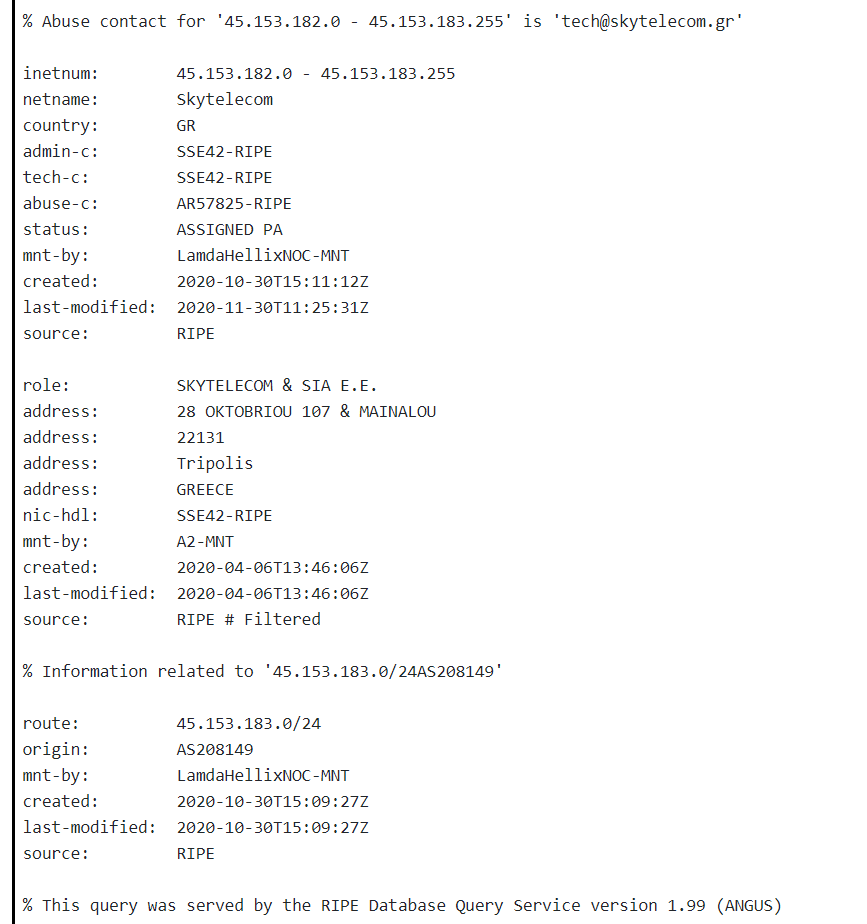
1. Looked up IP Address on virus total
2. Then looked it up on <https://www.whatismyip.com/ip-whois-lookup/>

* IP: 45.153.183.167

Virus total showed that it did not pick up on any malicious code. It also Identified that it belongs to Skytelecom & Sia E.e and is located in Greece

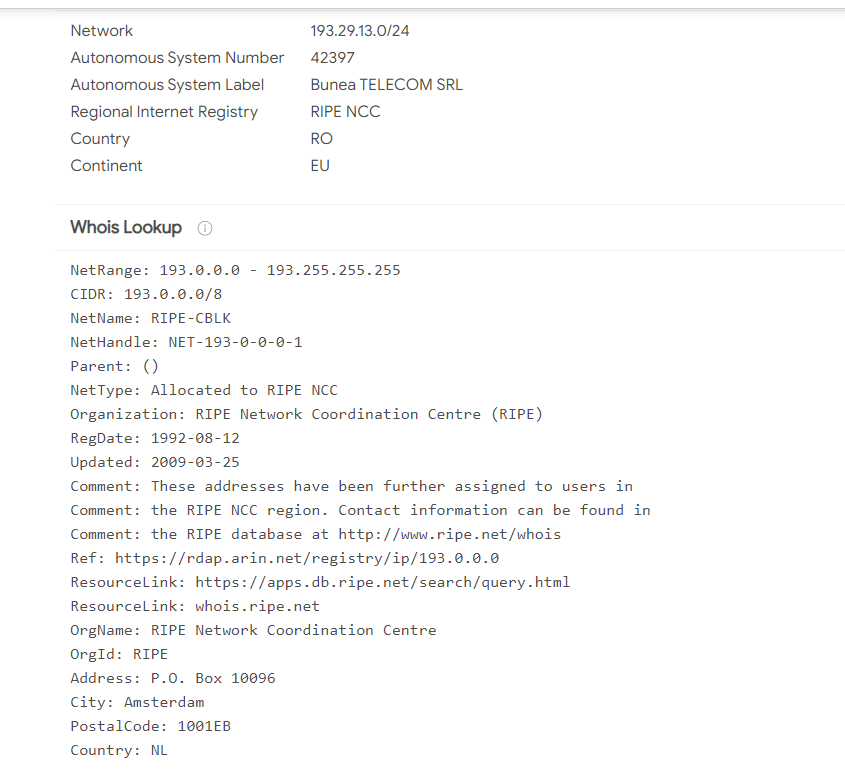
I found that between the IP’s of 45.153.182.0-45.153.183.255 belong to this company

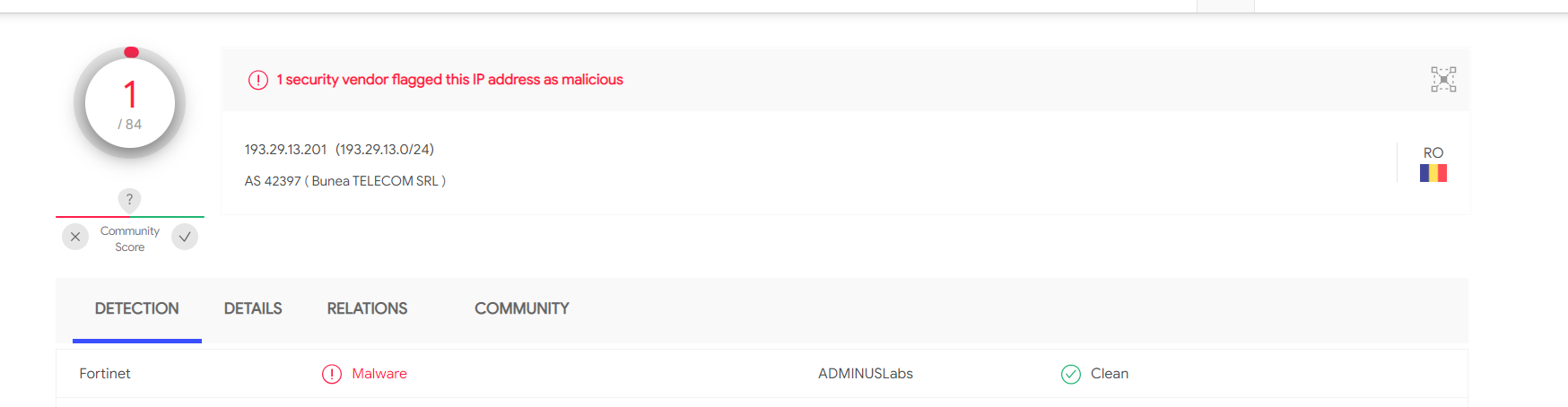
It was created on April 6, 2020 and last modified on the same date. I also found the IP address of the machine which is 28 Oktobriou 107 & Mainalou



-IP: 193.29.13.201

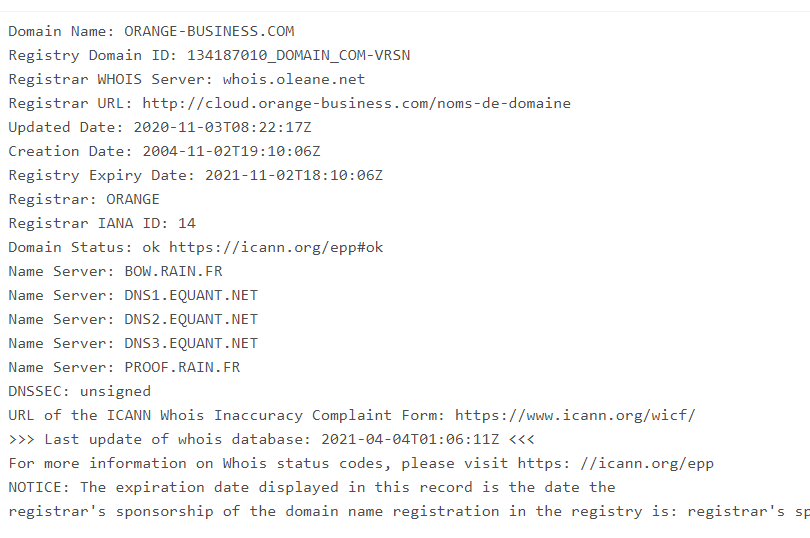
I found from virus total that it found malicious code on the page. I also found that the range of IP is 193.0.0.0 through 193.255.255.255. The name of the company is Bunea Telecom SRL and is in Amsterdam It was registered in 1992 August 12, and last updated on March 25, 2009.

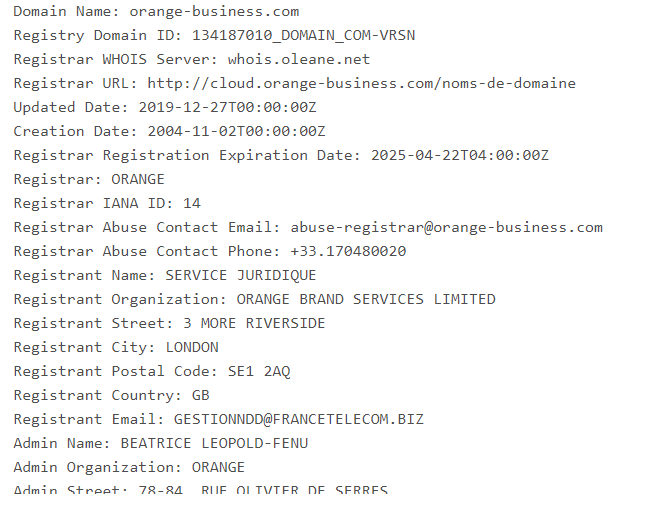


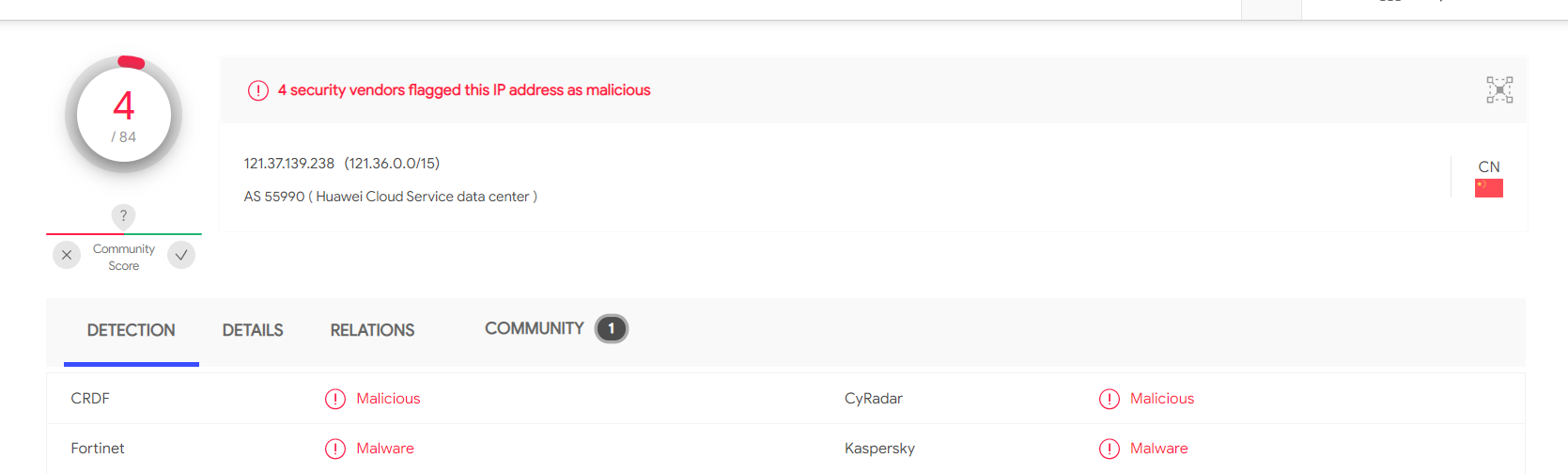


-121.37.139.238

4 different security vendors found malicious code. The Domain name according to both virusTotal and whatismyip website shows that is is orange-business.com Along with the admin name(Beatrice Leopold -Fenu), their email as well, and that it is located in London as well.

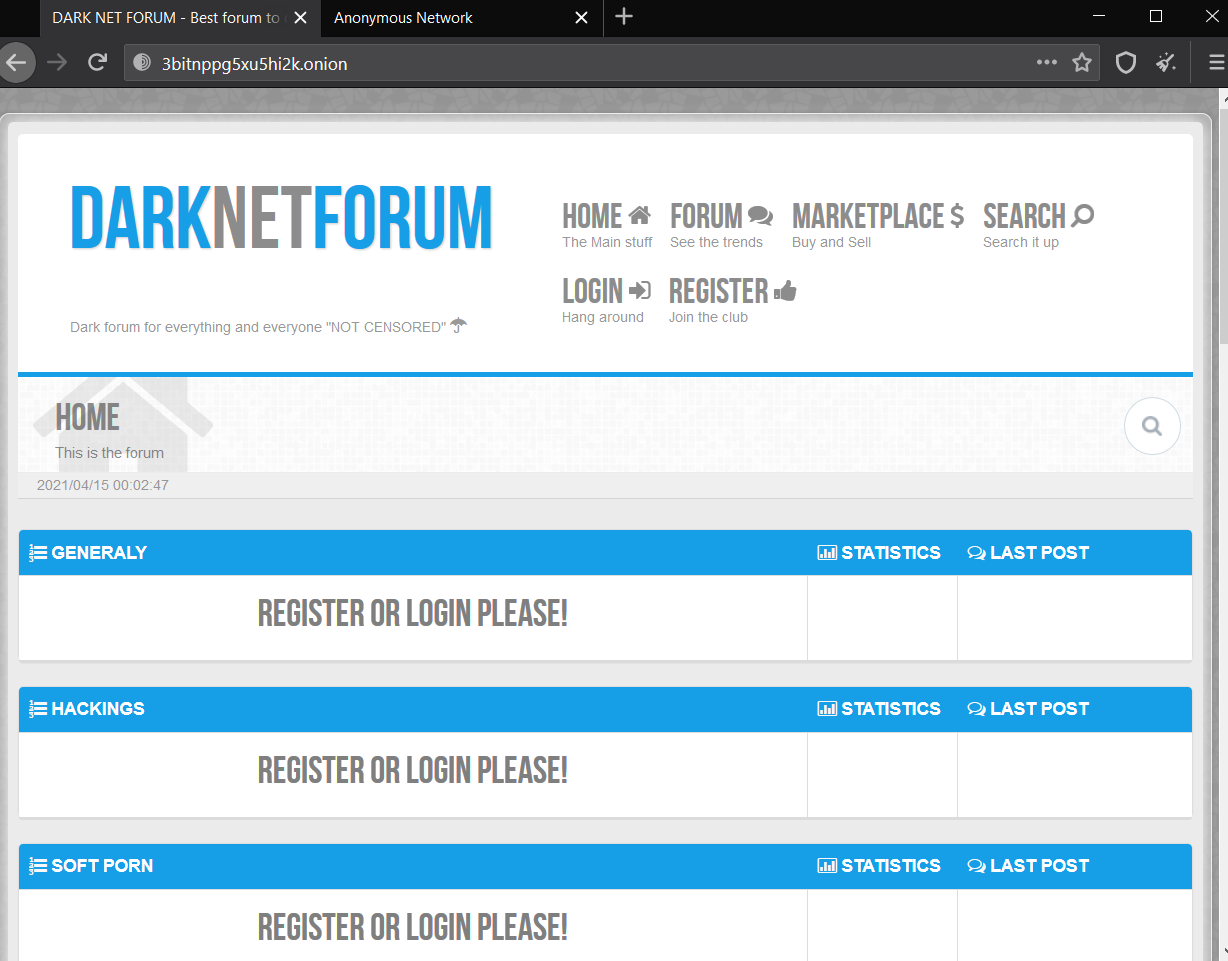






Onion websites

The first website(3bitnppg5xu5hi2k.onion) website is a forum website but will need to register or login



The second website is the website for Anonymous (hacker2twpebqewz.onion)

