ANALYZING THE DIGITAL CERTIFICATES OF DOMAIN NAMES USING OSINT TOOLS

BY

SOMKENE RICHARD

3rd NOVEMBER, 2024

EXECUTIVE SUMMARY

The digital certificates of the domains www.cyberagent.co.jp, www.thespargroup.com, and www.tesla.com were analyzed using OSINT tools including Virustotal, whoer.net and Abuseipdb, to verify the identity and authentication of these domains. The certificates were issued by reputable Certificate Authorities and showed valid expiration dates, with secure encryption standards in place. Alongside the certificates, the IP addresses of these domains were also examined, all of which corresponded, confirming the authentication of each domain. Additionally, the hosting providers and geolocation data aligned with the domains' verified identities, adding an extra layer of trustworthiness. In conclusion, the results suggest that these domains are secure and safe to interact with.

INTRODUCTION

Digital certificates, also known as SSL/TLS certificates, are electronic files that verify a website's identity and enable secure, encrypted connections between the site and its users. These certificates are issued by trusted third-party organizations called Certificate Authorities after confirming the website owner's identity.

Analyzing digital certificates is a proactive measure against cyberattacks, such as certificate spoofing, certificate authority compromise and others. This digital certificate analysis also helps identify vulnerabilities, like expired certificates.

TOOLS

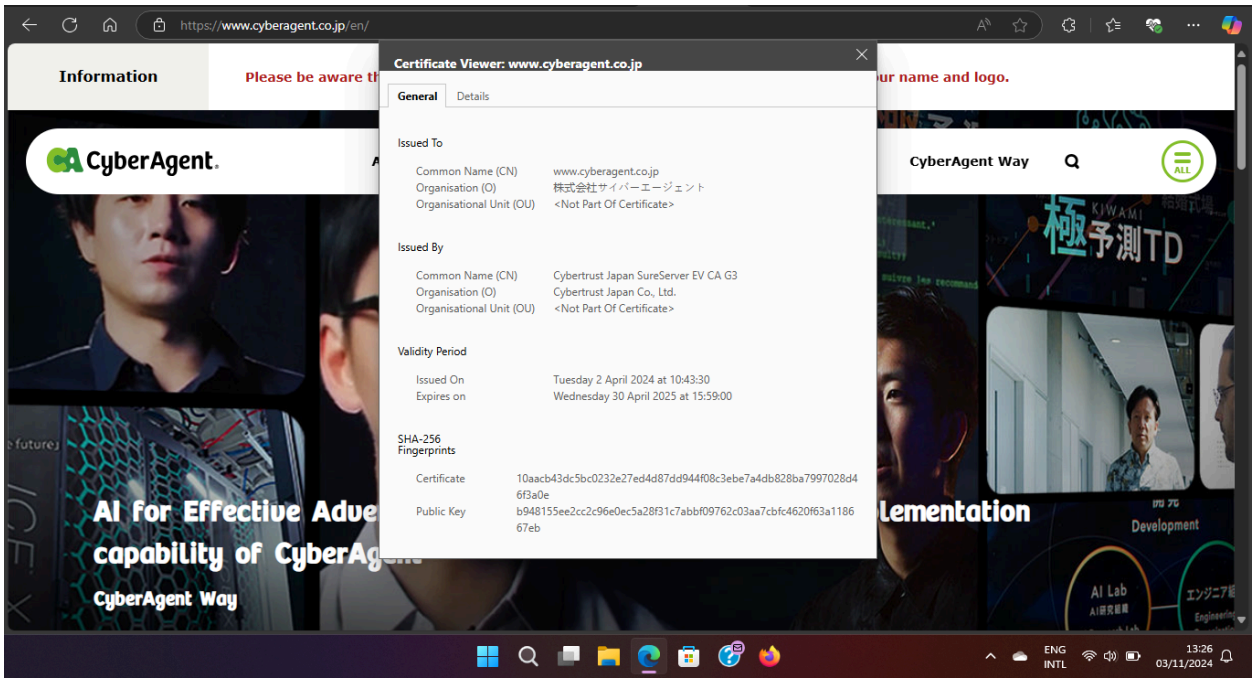
Virustotal

whoer.net

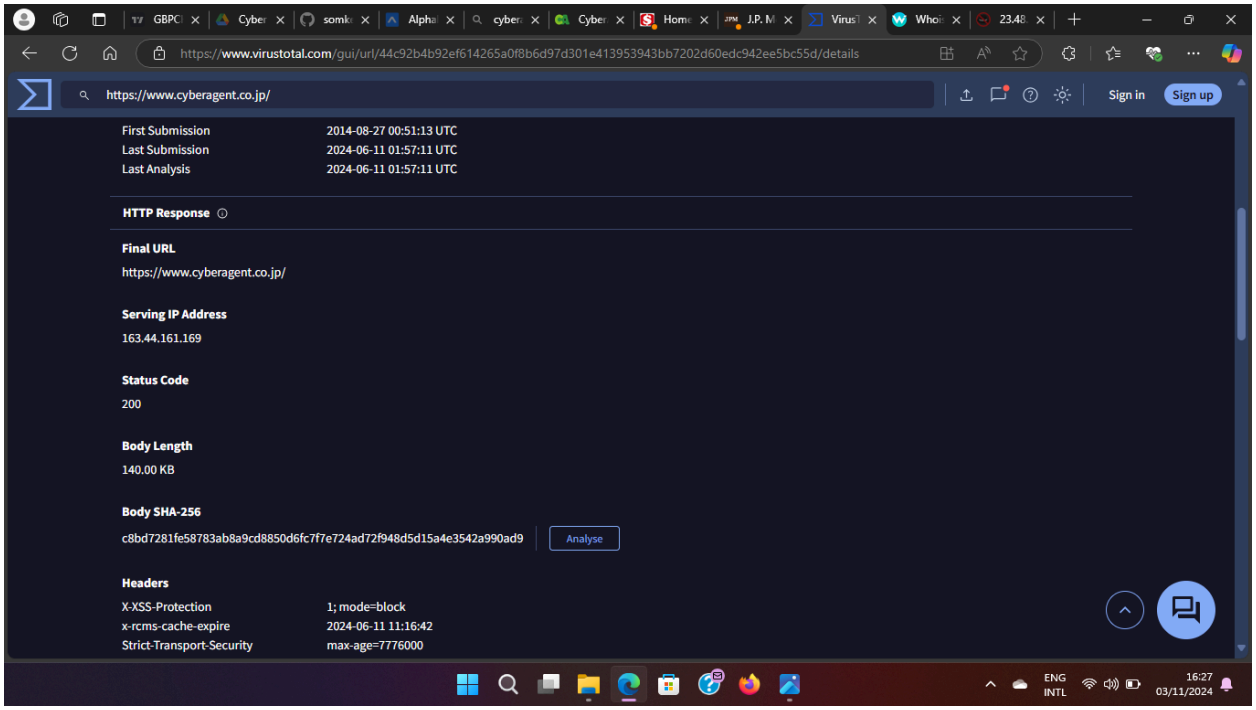
Abuseipdb

ANALYSIS

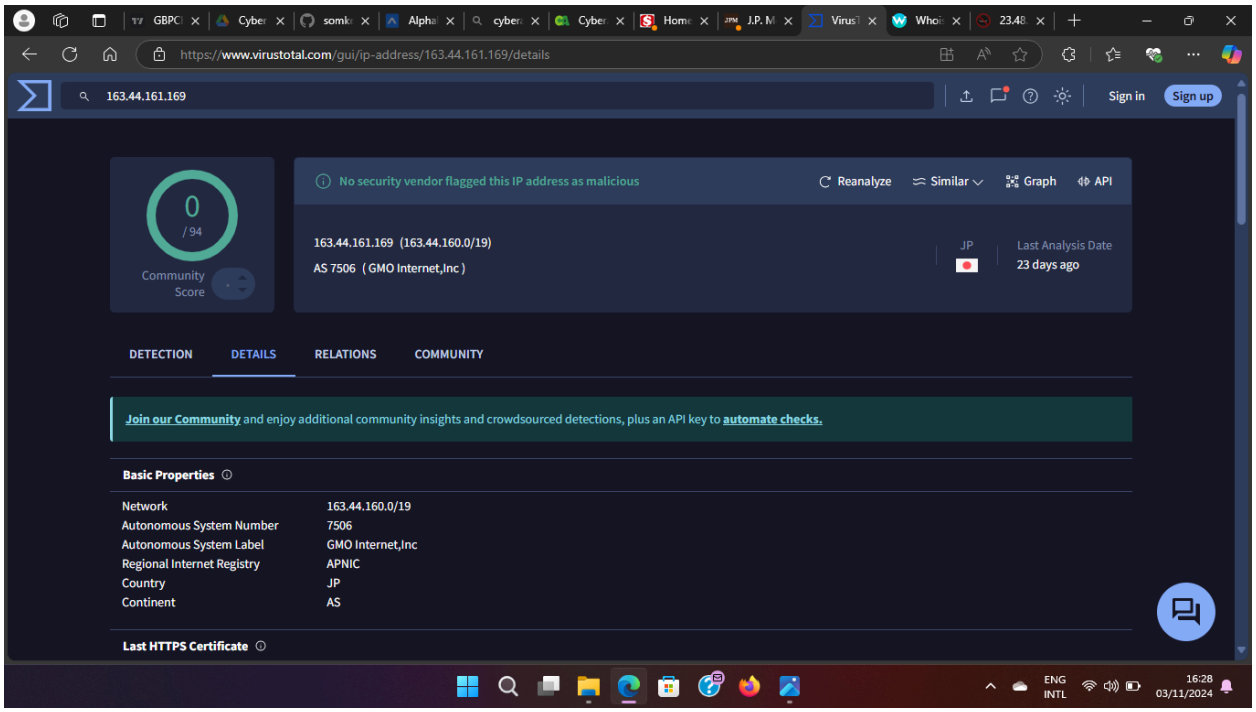
A. cyberagent.co.jp



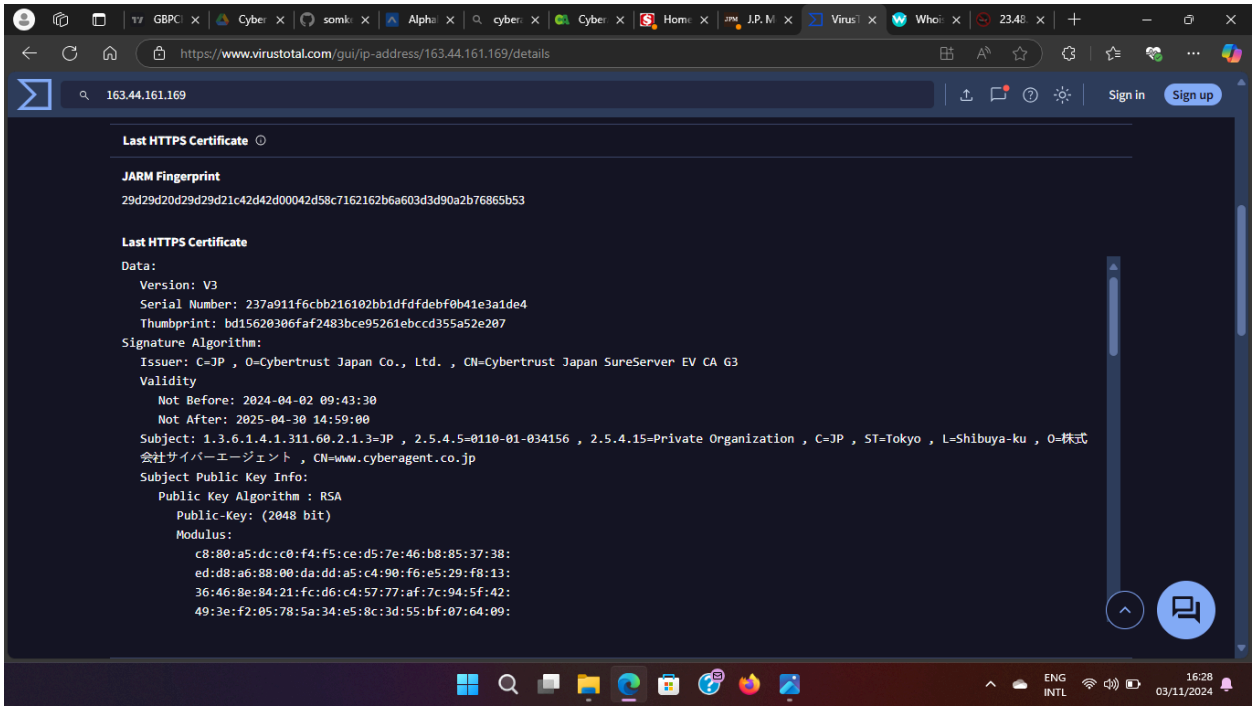
An Overview of the certificate viewer, showing important details of the website



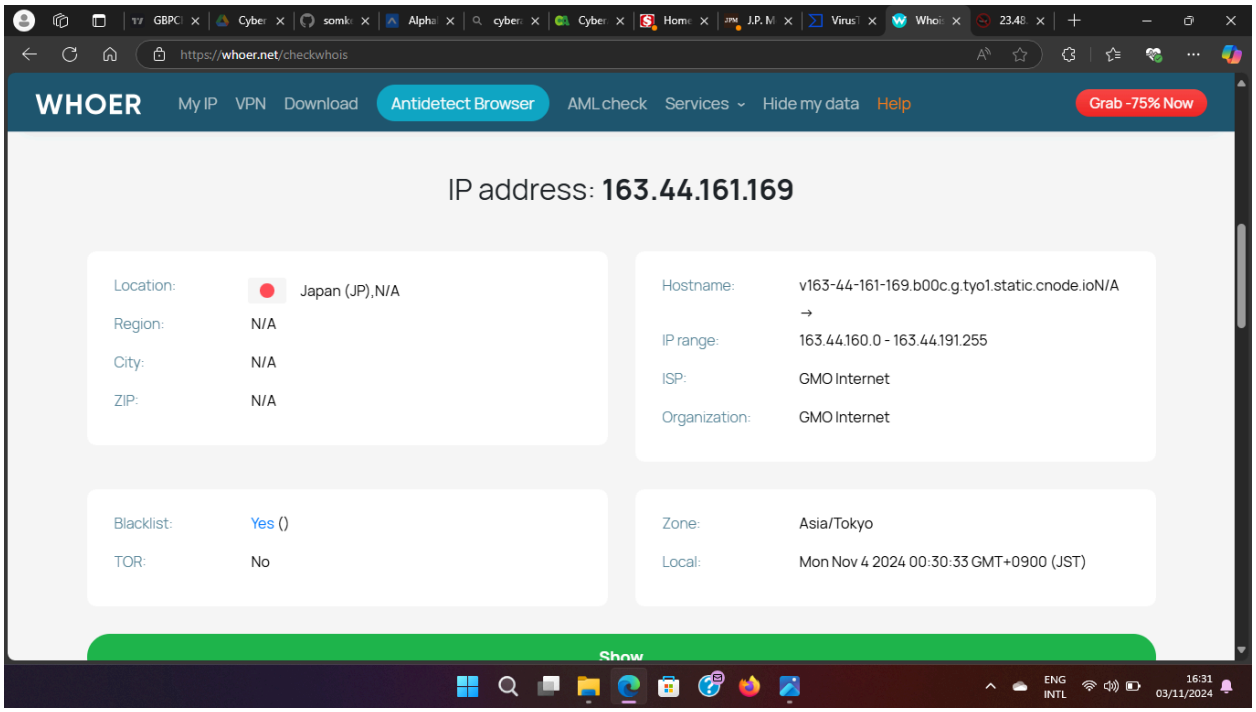
The url was scanned on virustotal.com to reveal its IP address (163.44.161.169)



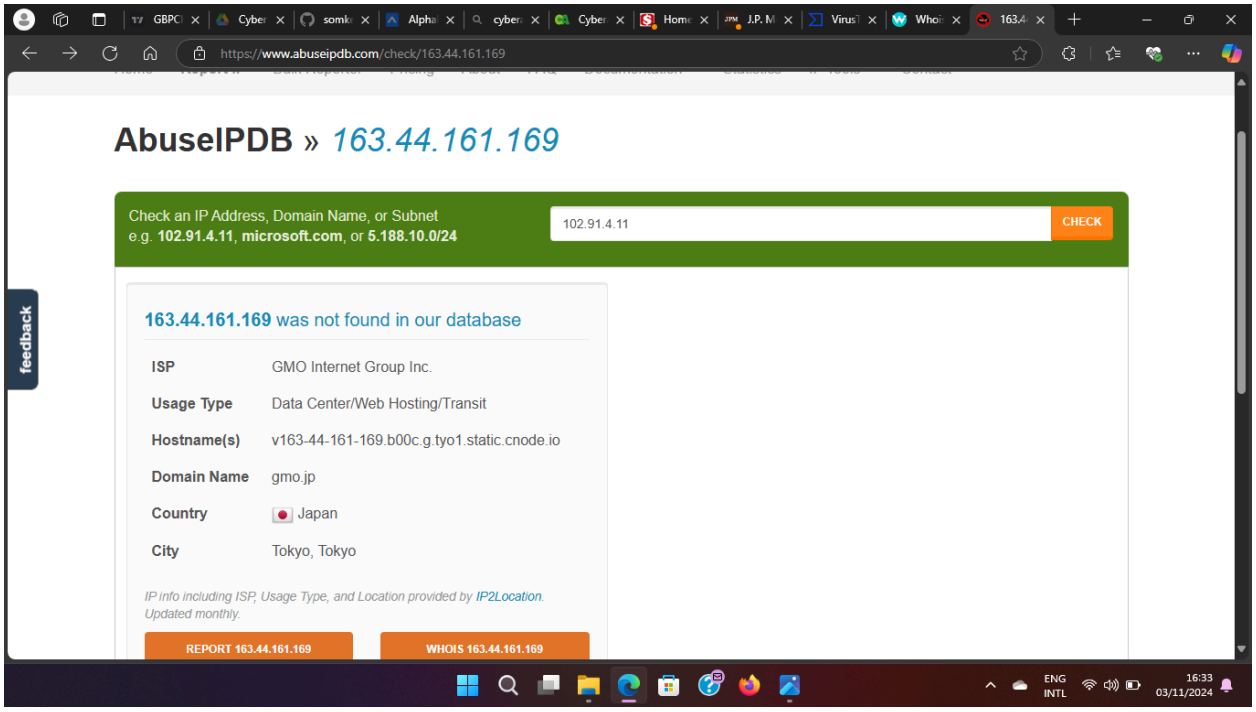
The IP was further scanned for more details of the domain



The scanned IP address shows the same certificate details as seen on the certificate viewer

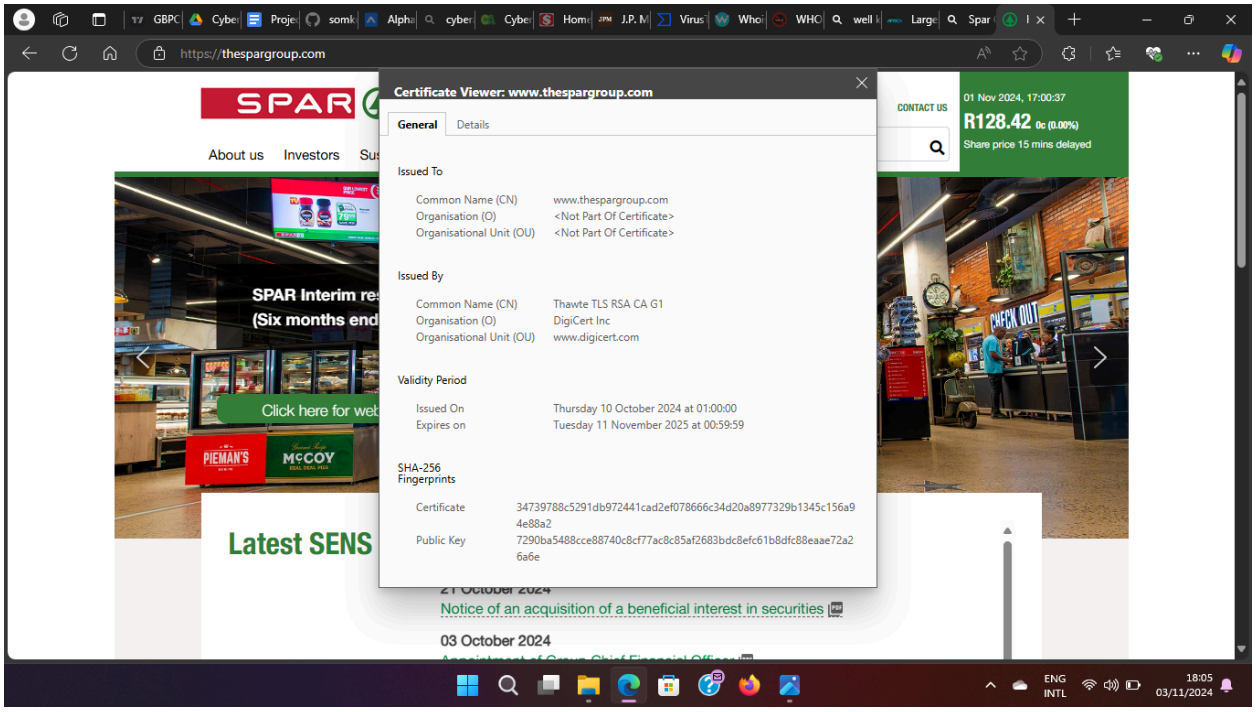


Further scanning on Whoer check for more verification and authenticity including its geolocation (Tokyo, Japan)

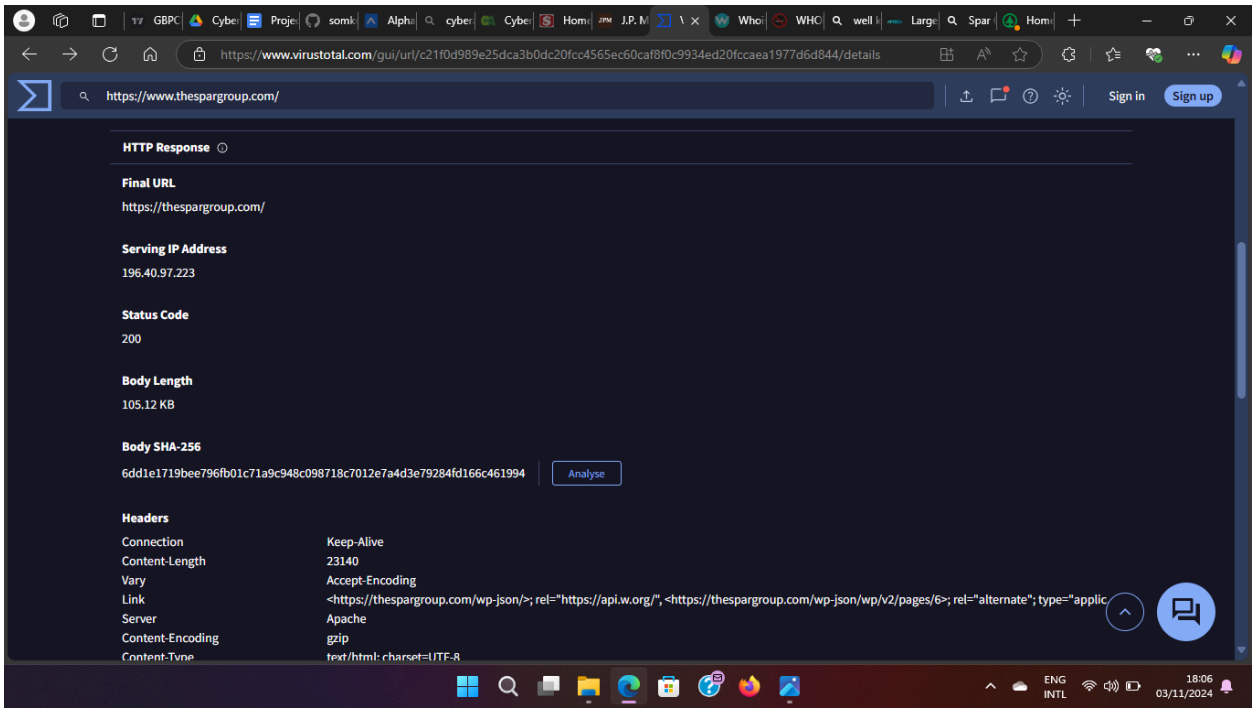


The IP wasn't found in abuseipdb database, meaning that no report of malicious activities has been reported of it yet . Other details shows its correspondence with whoer.net

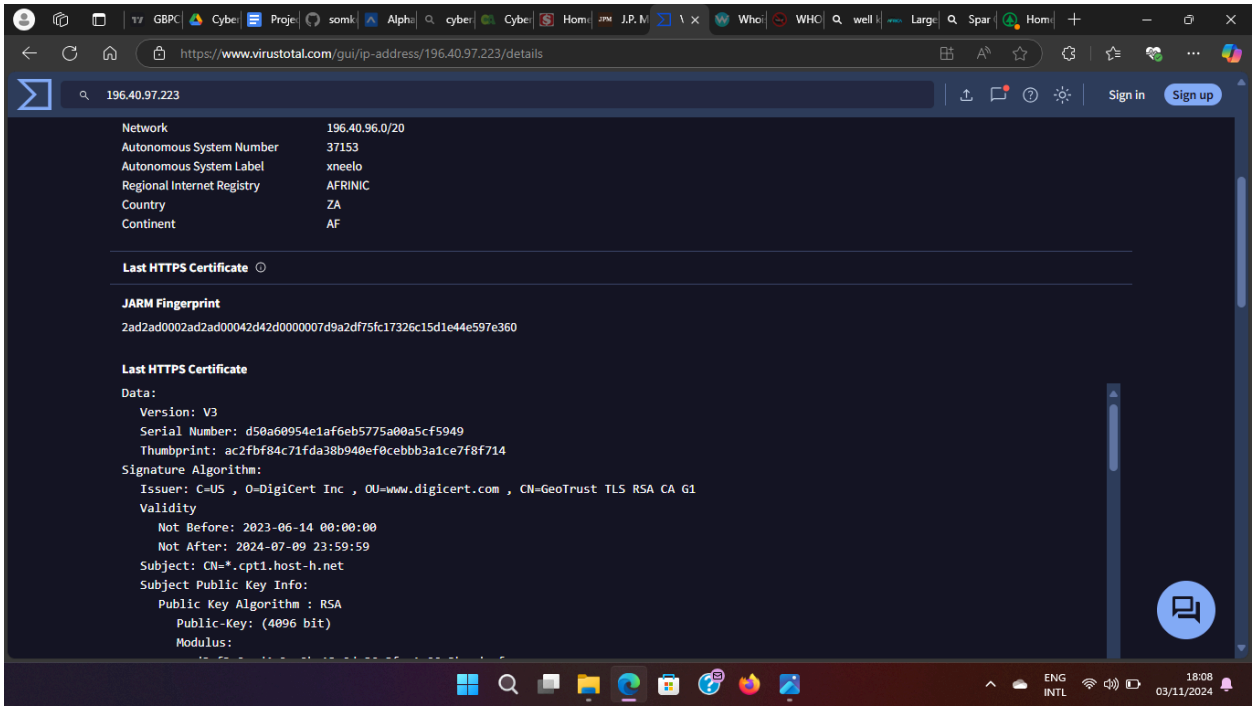
B. Thespargroup.com



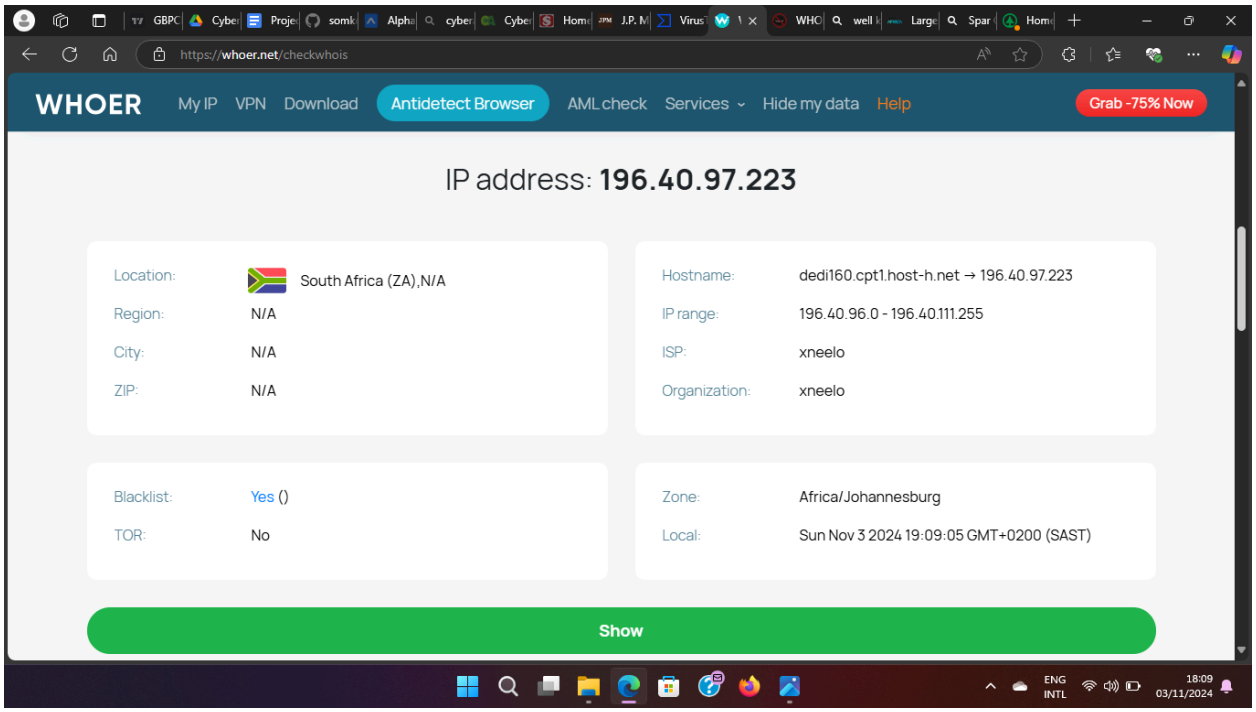
An Overview of the certificate viewer, showing important details of the website



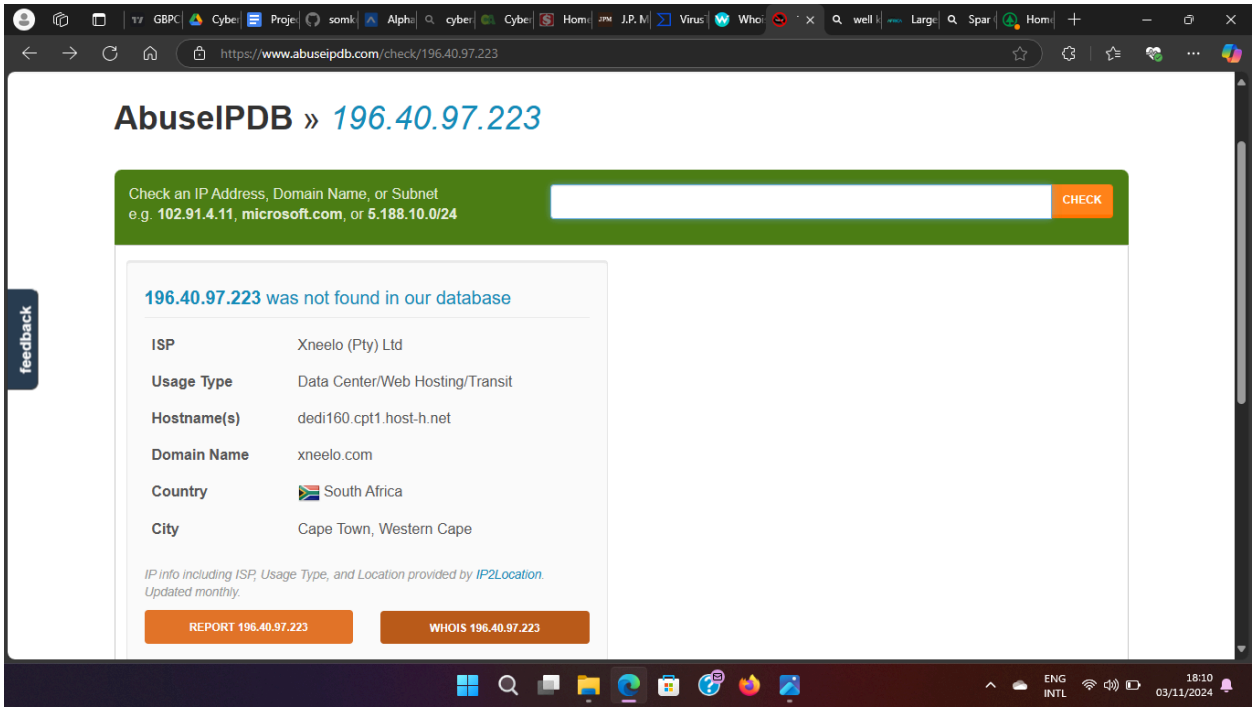
The url was scanned on virustotal.com to reveal it's IP address (196.40.97.223)



The IP address was further scanned, and its certificate details corresponded with the one seen on the certificate viewer

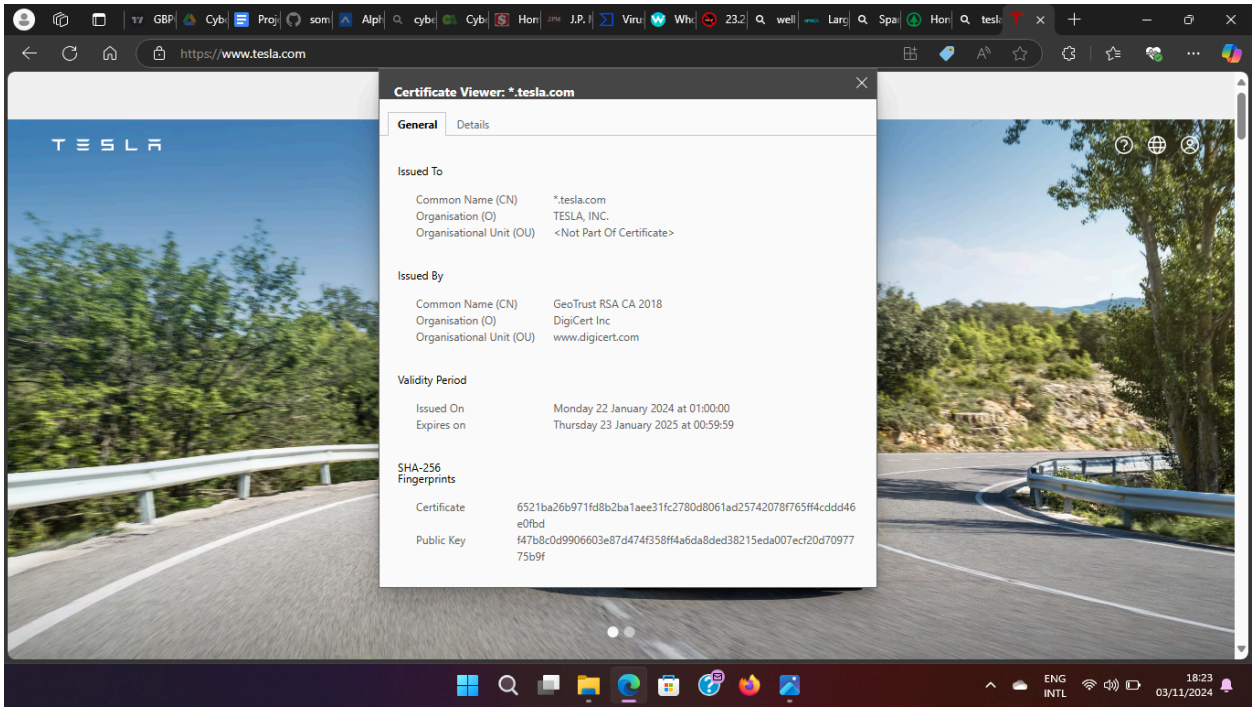


Further scanning on whoer.net revealed more details of the domain including its geolocation (Johannesburg, SouthAfrica)

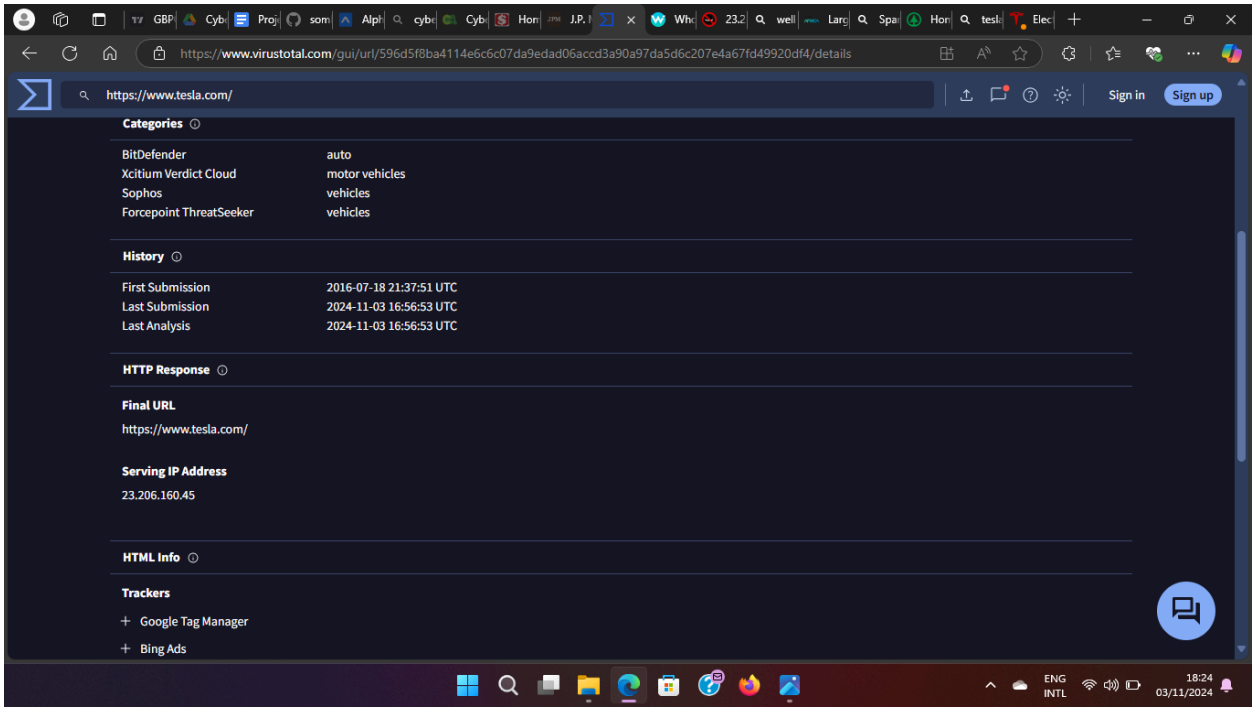


Scanning on abuseipdb showed the IP address has not been reported for any malicious activity

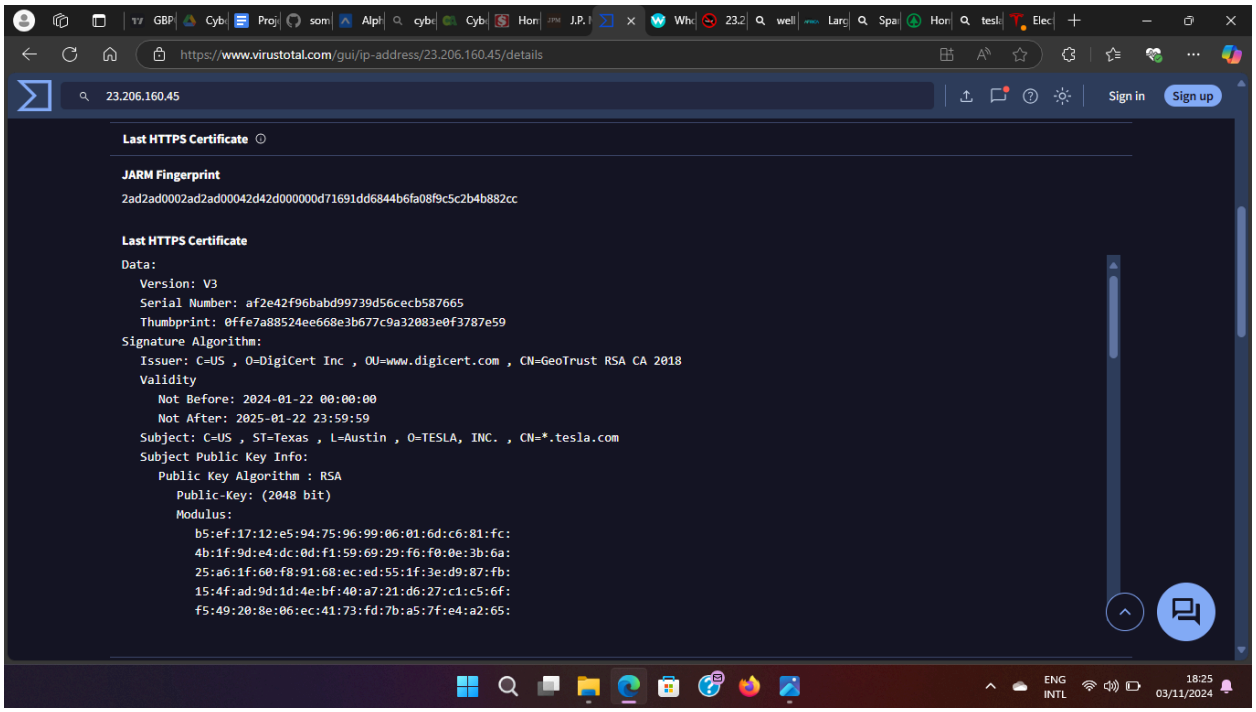
C. Tesla.com



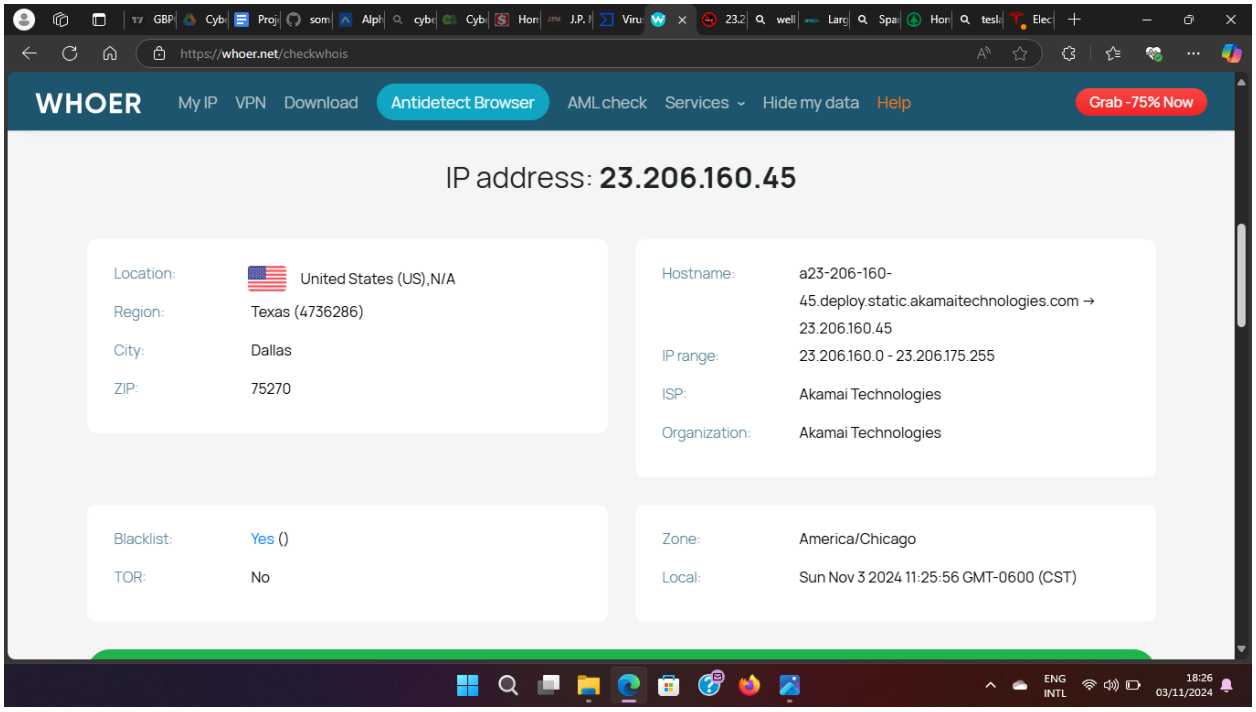
An Overview of the certificate viewer, showing important details of tesla.com



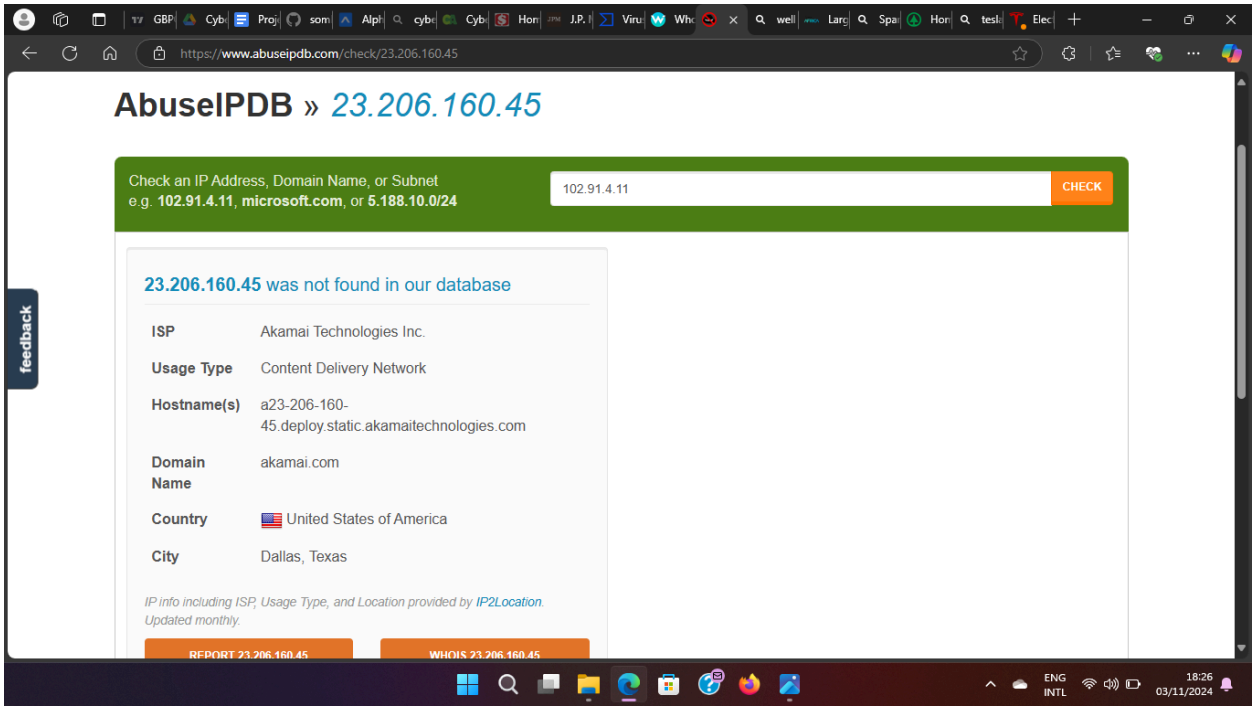
The url was scanned on virustotal.com to reveal its IP address (23.206.160.45)



The IP address was further scanned and the certificate details corresponded with that seen on the website's certificate viewer



Further scanning on whoer.net revealed more details about the IP address including its geolocation (Texas, U.S.A)



The IP address wasn't found on abuseipdb indicating that its hasn't been reported for any malicious activity or attempt

RECOMMENDATION

1. The respective organizations should endeavor to renew their certificates as and when due.
2. The cryptographic algorithms used in securing the domains should be evaluated and updated continually to ensure maximum data encryption.
3. Additional security measures like multi-factor authentication, Intrusion Detection and Prevention systems should not be left out for further strengthening of data protection.

CONCLUSION

In conclusion, the analysis results show a high confidence in the domain authenticity respectively and therefore are safe to interact with. However, Subsequent and deeper analysis can be done as well to prevent any vulnerability that could lead to potential cyberattacks ranging from certificate spoofing, Certificate authority compromise , etc