HTTP TRAFFIC ANALYSIS AND DOMAIN INVESTIGATION USING WIRESHARK, VIRUSTOTAL, AND WHOER.NET

BY

SOMKENE RICHARD

21st SEPTEMBER, 2024

EXECUTIVE SUMMARY

An analysis of network traffic on http://altoromutual.com identified a critical security risk. This analysis, utilizing Wireshark for packet capture, revealed that login credentials are being transmitted in plain text.

This lack of encryption, due to the use of an unencrypted HTTP protocol, exposes user data to potential interception by a threat actor.

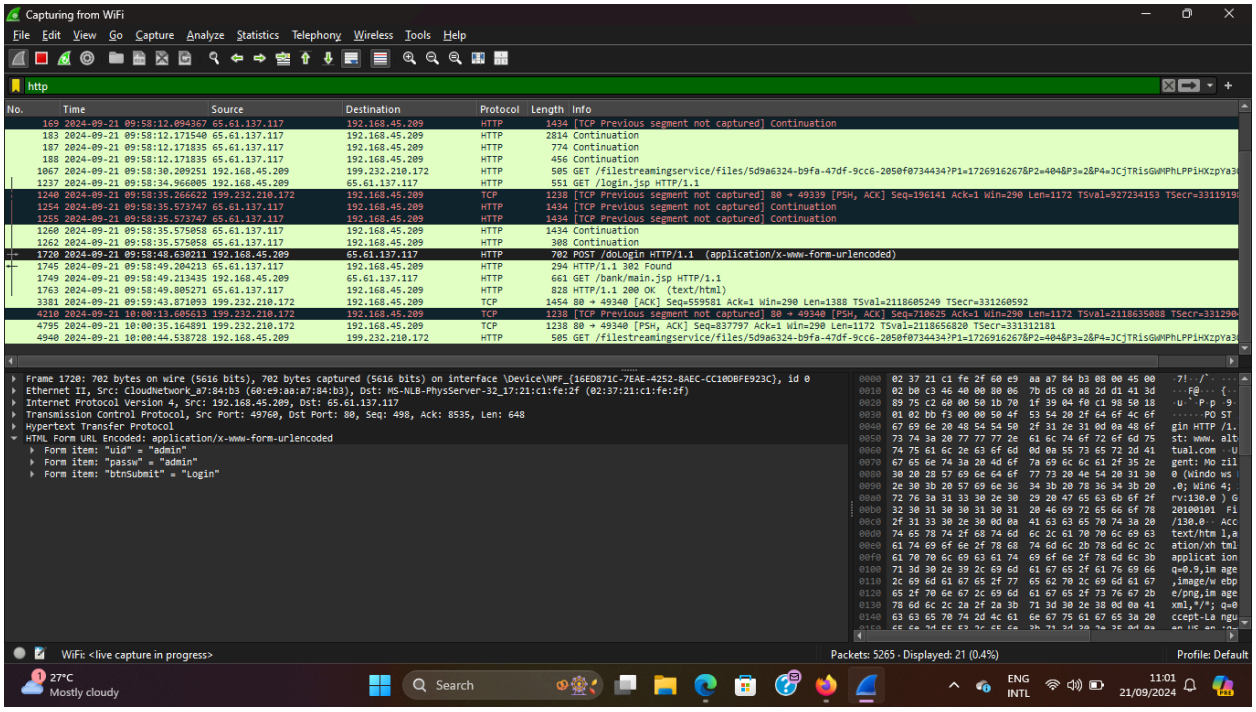
INTRODUCTION

Encryption plays a crucial role in keeping data safe from unauthorized access and interception. Many websites now use HTTPS to secure and encrypt information entered by users. However, attackers can still create fake versions of these sites using the less secure HTTP protocol. When users unknowingly interact with these fraudulent sites, their login details and other sensitive information can be exposed and exploited by cybercriminals.

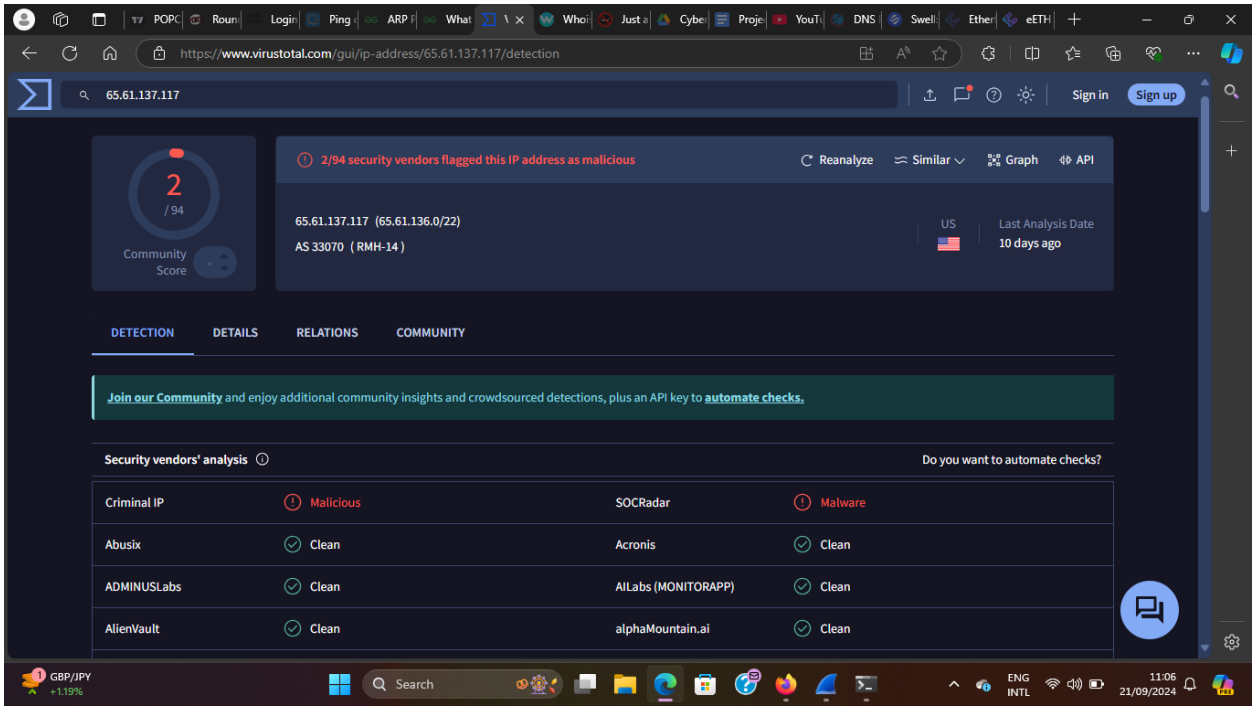
TOOLS

1. Wireshark
2. Whoer.net
3. Abuseipdb
4. Pen and paper

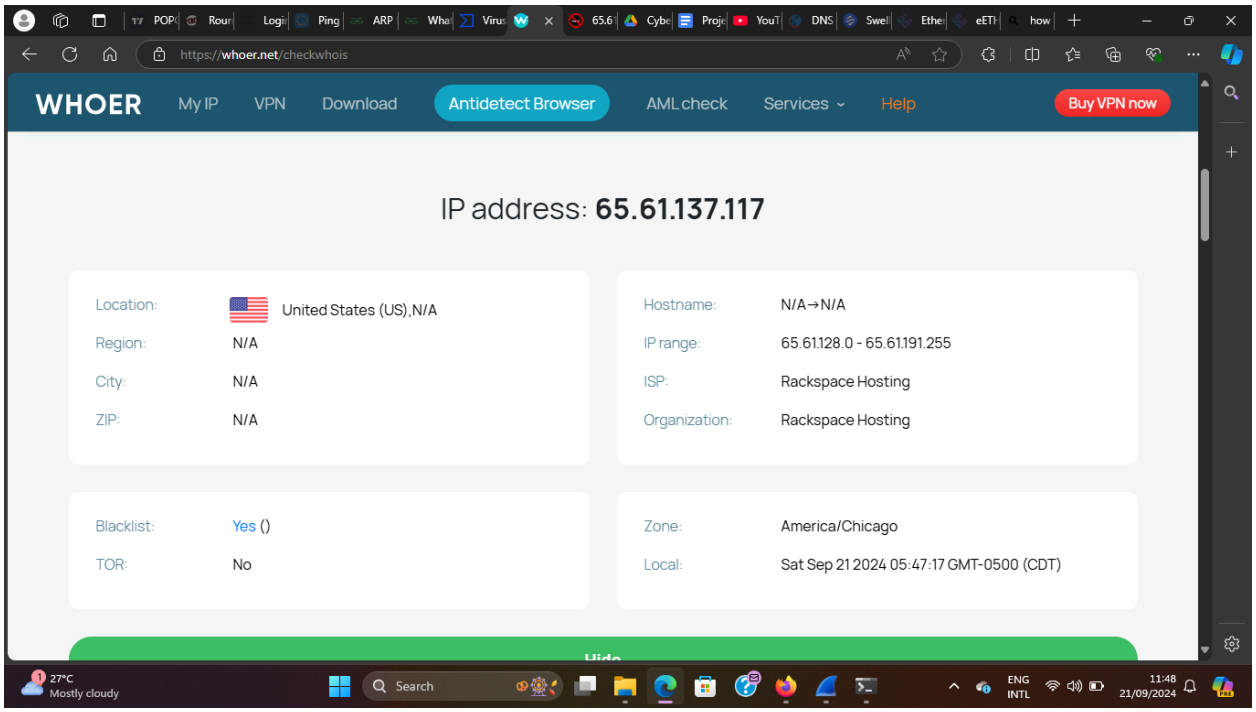
ANALYSIS



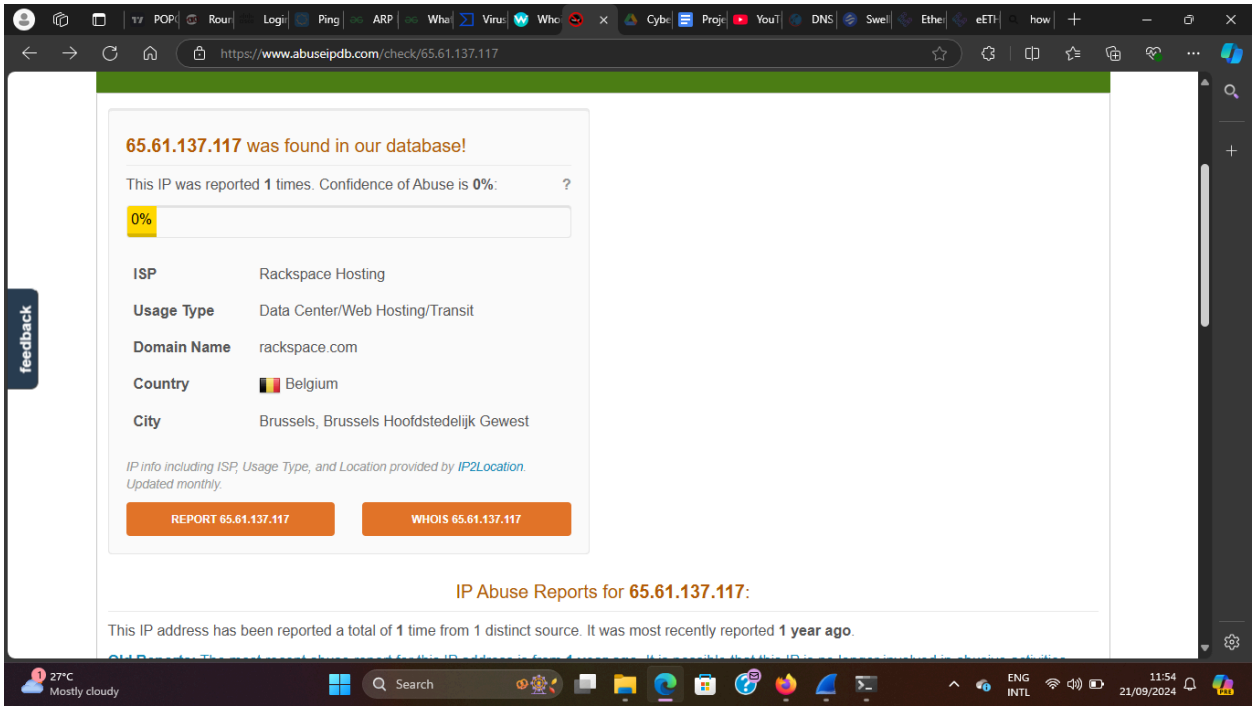
From the image above, the login details could be seen as a plaintext under "uid" and "passw" due to the HTTP protocol



on virustotal, the IP address of the domain was flagged malicious by 2 security vendors



On Whoer.net, the location of the domain could be seen including the ISP and organization



Further scanning on abuseipdb shows that the IP address of the domain has been reported once about a year ago.

RECOMMENDATIONS

Based on my analysis, I'd recommend the following:

1. Temporarily disabling the login functionality on the website until a secure HTTPS connection is implemented. This would prevent further exposure of user credentials.
2. To address the malicious flagging and reports of the IP address, the domain owner(s) should investigate and resolve the underlying security issues that are causing these flags.
3. Implement a security awareness training program to educate users on how to identify and avoid insecure websites (HTTP) and encourage safe online practices.

CONCLUSION

The domain was found to be insecure, as it exposes users' login credentials, making them vulnerable to interception by threat actors. This issue can be addressed by using secure domains that implement HTTPS encryption, which significantly reduces the risk of data exposure compared to HTTP connections.