### **Phishing Analysis**

This blog is a walkthrough of the Phishing Analysis challenge at [BTLO](http://blueteamlabs.online).

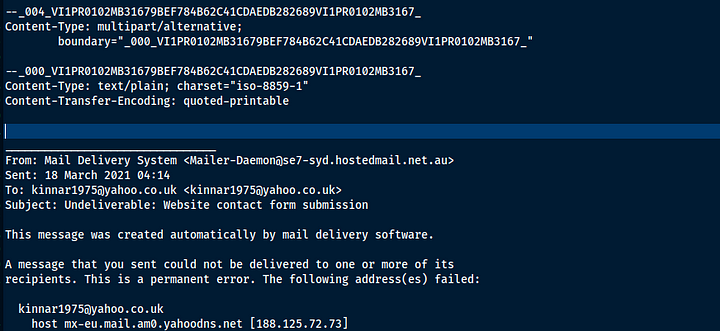
**Scenario:** A user has received a phishing email and forwarded it to the SOC. Can you investigate the email and attachment to collect useful artifacts?

Download the given zip file and extract the contents using the given password — “btlo”.

#### **Tasks**

1. **Who is the primary recipient of this email?**

Let us open the given .eml file in text editor. To find the primary recipient we can look at the To field in the email headers.

email header

Answer: kinnar1975@yahoo.co.uk

**2.What is the subject of this email?**

The subject can be seen in the above screenshot in the subject field.

**Answer:** Website contact form submission

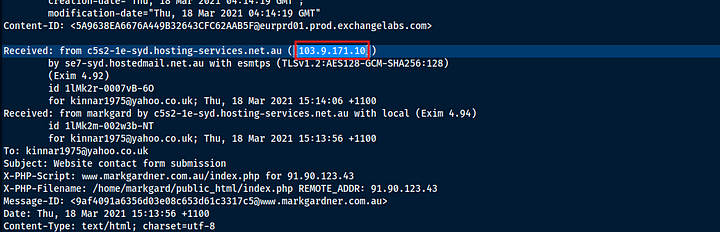
**3.What is the date and time the email was sent?**

This can also be seen in the previous screenshot under the Date field.

**Answer:** 18 Mar 2021 04:14

**4.What is the Originating IP?**

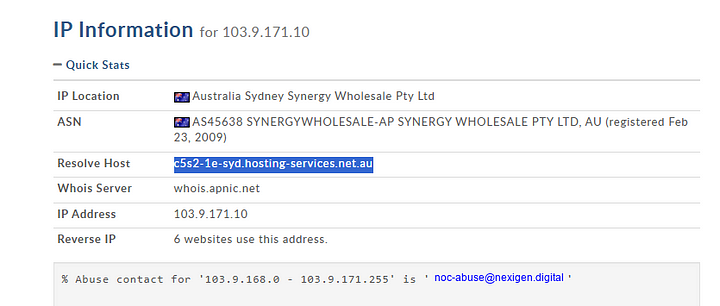
This information can usually be found in the most recent received headers. which means that the sender IP can be found in the received headers closest to the message

received header

Answer: 103.9.171.10

**5.Perform reverse DNS on this IP address, what is the resolved host?**

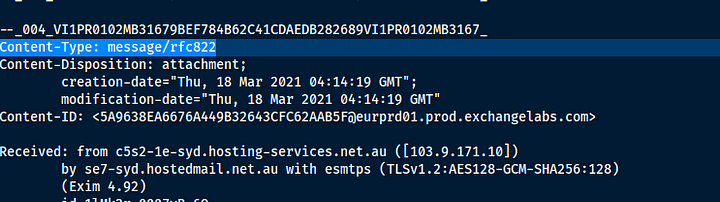
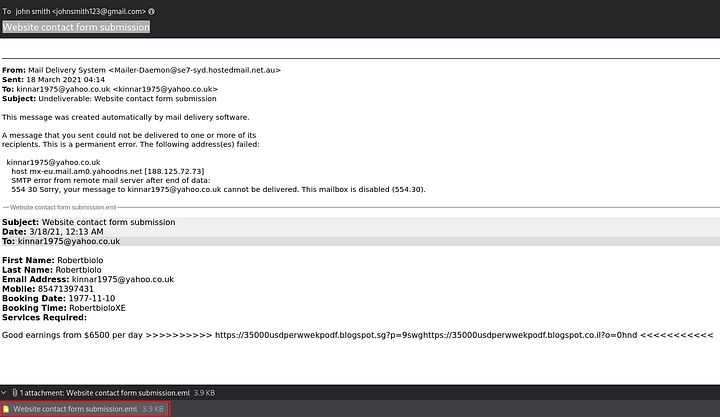
The resolved host address can be seen in the above screenshot, but we can also find this using online tool called the Whois domain lookup tool which can be used at<https://whois.domaintools.com/>

Whois domain lookup

**Answer:** c5s2–1e-syd.hosting-services.net.au

**6.What is the name of the attached file?**

To check this we need to open the email in a Mail User Agent(MUA) as this information is not present in the metadata for this email. In the metadata it is mentioned that the content type is message/rfc822 which is an email. Hence the attachment should be an email file.

email header showing the attachment typeMUA

**Answer:** Website contact form submission.eml

**7.What is the URL found inside the attachment?**

This is visible in the above screenshot.

**Answer:** hxxps[://]35000usdperwwekpodf[.]blogspot[.]sg?p=9swghxxps[://]35000usdperwwekpodf[.]blogspot[.]co[.]il?o=0hnd

**8.What service is this webpage hosted on?**

This is evident form the URL.

**Answer:** BlogSpot

**9.Using URL2PNG, what is the heading text on this page? (Doesn’t matter if the page has been taken down!)**

**Answer:** Blog has been removed

