Blue Team Labs Online: Phishing Analysis

The following writeup is for Phishing Analysis on Blue Team Labs Online, it's an easy lab that involves analysing a raw phishing email through using tools like a text editor, Mozilla Thunderbird, and more. This was a super easy email analysis, you don't required any specialised knowledge, only a basic understanding of email headers.

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?

Who is the primary recipient of this email?

Before I dive into this question, it is important to remind everyone that you should only analyse this email and its artifacts within a sandboxed environment, in my case I am using Remnux for any attachment analysis. To start the investigation, I am going to be using Sublime text along with EmailHeader syntax plugin created by 13Cubed:

```
From: Mail Delivery System <Mailer-Daemon@se7-syd.hostedmail.net.au>
Sent: 18 March 2021 04:14
To: kinnar1975@yahoo.co.uk <kinnar1975@yahoo.co.uk>
Subject: Undeliverable: Website contact form submission
```

Answer: kinnar1975@yahoo.co.uk

What is the subject of this email?

```
From: Mail Delivery System <Mailer-Daemon@se7-syd.hostedmail.net.au>
Sent: 18 March 2021 04:14
To: kinnar1975@yahoo.co.uk <kinnar1975@yahoo.co.uk>
Subject: Undeliverable: Website contact form submission
```

Answer: Undeliverable: Website contact form submission

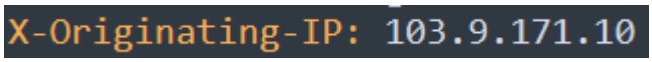
What is the date and time the email was sent?

```
From: Mail Delivery System <Mailer-Daemon@se7-syd.hostedmail.net.au>
Sent: 18 March 2021 04:14
To: kinnar1975@yahoo.co.uk <kinnar1975@yahoo.co.uk>
Subject: Undeliverable: Website contact form submission
```

Answer: 18 March 2021 04:14

What is the Originating IP?

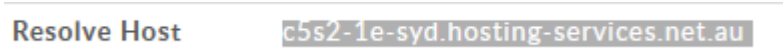
The X-Original-IP field is a custom email header that identifies the IP address of the client that originally initiated the connection to a mail service. The IP can be found near the end of the raw file:



Answer: 103.9.171.10

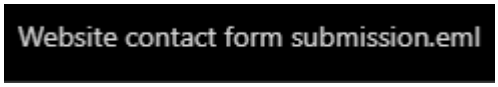
Perform reverse DNS on this IP address, what is the resolved host? (whois.domaintools.com)

I am going to use the provided tool, but you can always just use the whois command:



Answer: c5s2-1e-syd.hosting-services.net.auD

What is the name of the attached file?



Answer: Website contact form submission.eml

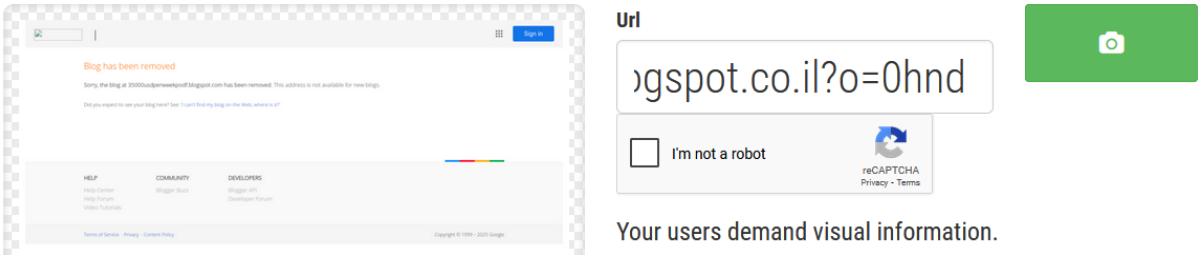
What is the URL found inside the attachment?

Answer: https://35000usdperwwekpodf.blogspot.sg/?p=9swghttps://35000usdperwwekpodf.blogspot.co.il?o=0hnd

What service is this webpage hosted on?

Answer: blogspot

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



Answer: blag has been removed