The Greenholt Phish

TryHackMe Challenge

Write-Up

Pavel Pecheniuk

1. Introduction

This room offers an opportunity to practice phishing email analysis skills in a lab environment. Phishing is the most common social engineering attack that forces people to disclose personal and sensitive information, such as login credentials, that perpetrators need to perform their malicious activity.

2. Scenario

A Sales Executive at Greenholt PLC received an email that he didn't expect to receive from a customer. He claims that the customer never uses generic greetings such as "Good day" and didn't expect any amount of money to be transferred to his account. The email also contains an attachment that he never requested. He forwarded the email to the SOC (Security Operations Center) department for further investigation.

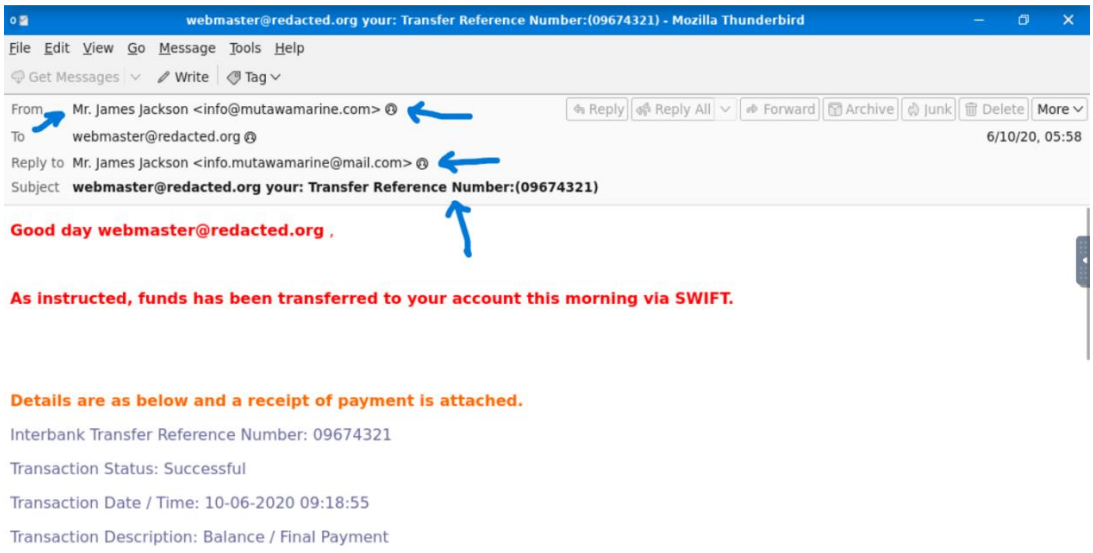
Investigate the email sample to determine if it is legitimate.

3. Investigation

What is the Transfer Reference Number listed in the email's Subject? Who is the email from? What is his email address? What email address will receive a reply to this email?

These questions are separate in the THM room, however I united them all in one since this is the information that can be found by exploring the email and the mail client.

The interesting part here are the different emails under *From* and *Reply to*. The fact that an employee received this email from one address but a response should go to the other is already suspicious.

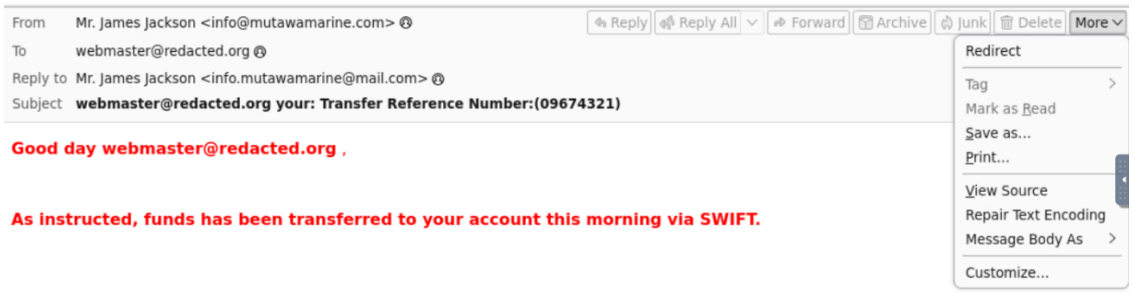


Answer:

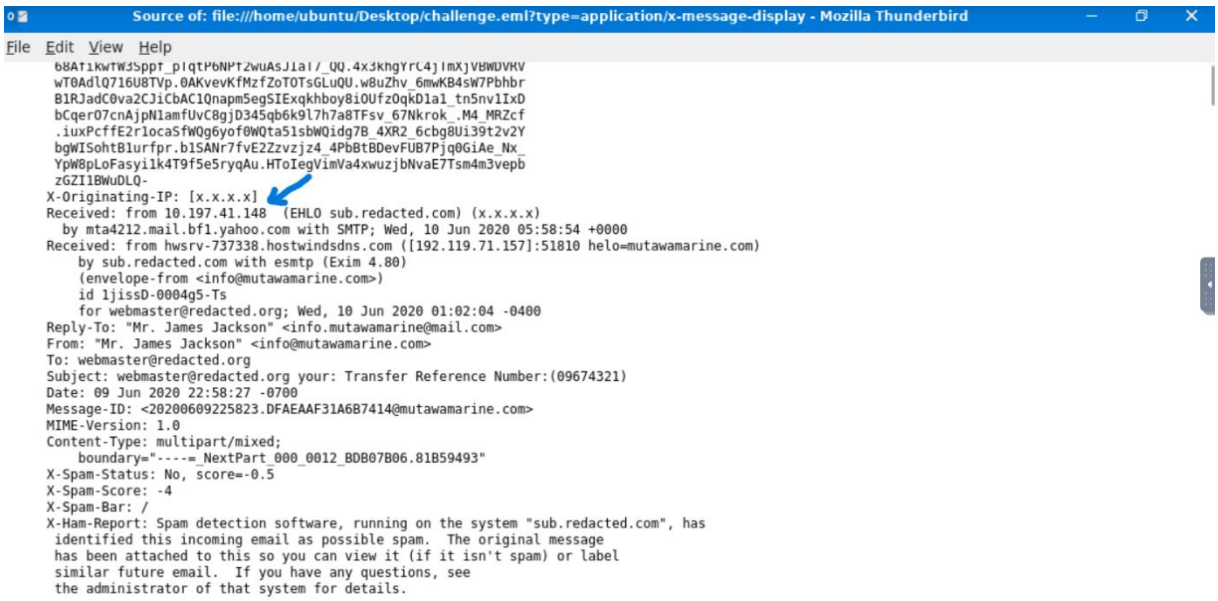
- 09674321
- Mr. James Jackson
- info@mutawamarine.com
- info.mutawamarine@mail.com

What is the Originating IP?

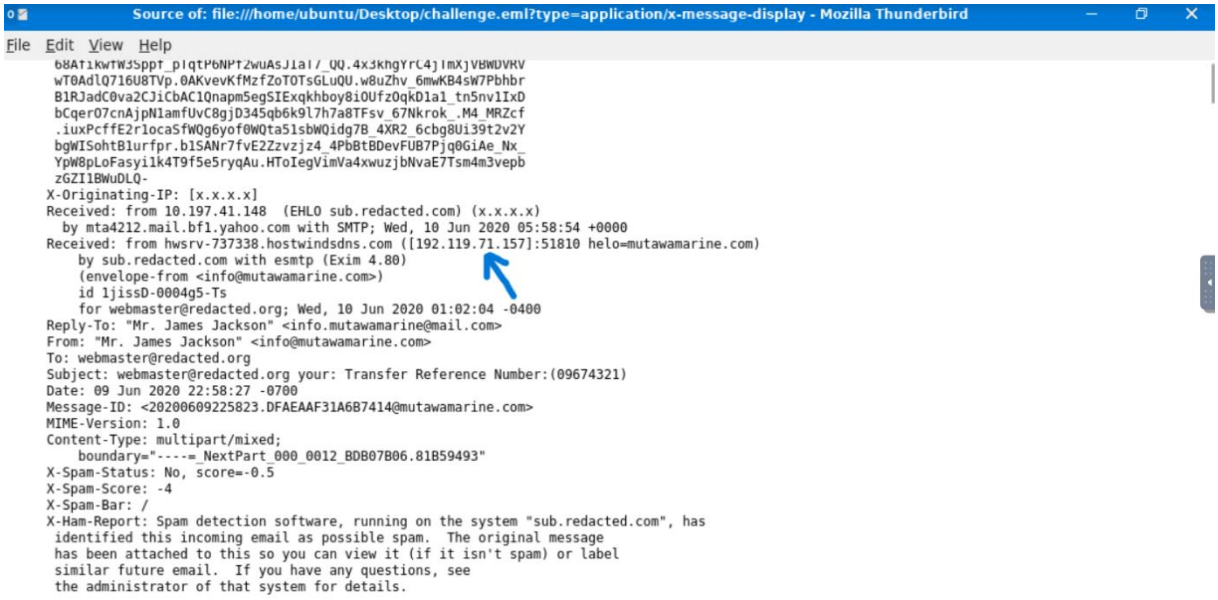
Let's find more information about the source. Navigating to it is done by selecting *More* > *View Source*.



We can see that *X-Originating-IP* is *10.197.41.148*. This is a private IP address, since it lies in the range *10.0.0.0 –10.255.255.255*. A private IP address is used by devices inside an internal network, so it cannot be reached directly from the public internet. To make it, a private address is translated to a public address via NAT (Network Address Translation) by router to access the global network. Hence, this is not the address we are looking for.



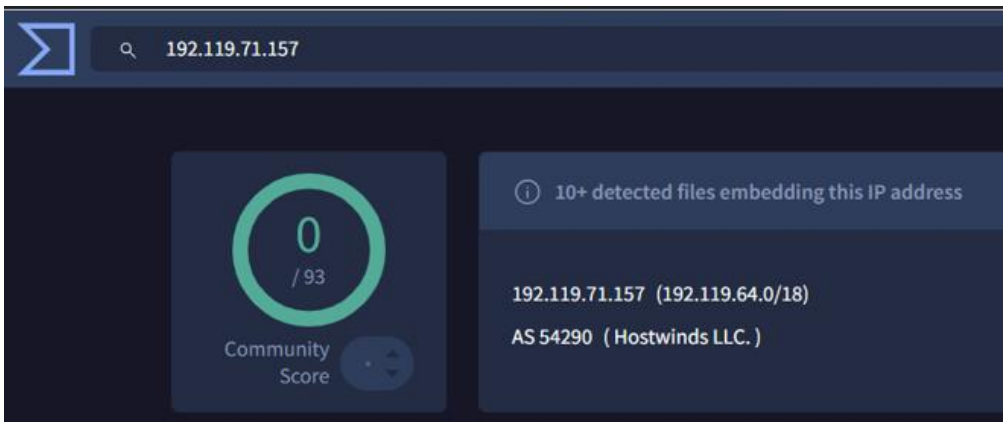
192.119.71.157 is the address we need since it is public and doesn't fall inside the ranges that usually indicate private IP addresses such as: *10.0.0.0 – 10.255.255.255*, *172.16.0.0 –172.31.255.255*, *192.168.0.0 –192.168.255.255*. It also appears in the *Received* header, indicating the true source of the email.



Answer: 192.119.71.157

Who is the owner of the Originating IP?

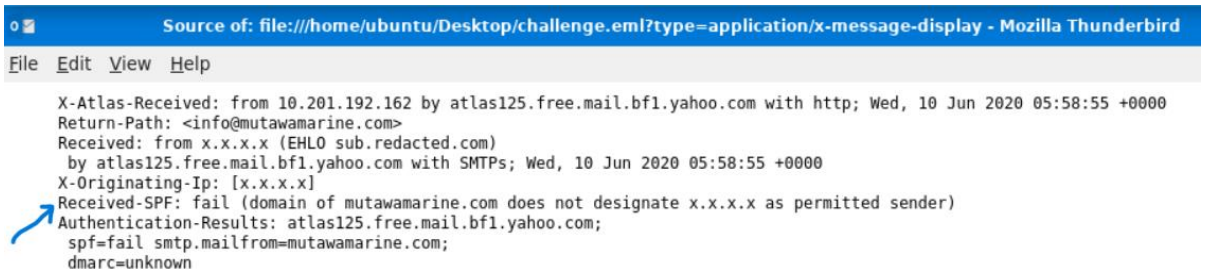
Let's research this IP address via VirusTotal.



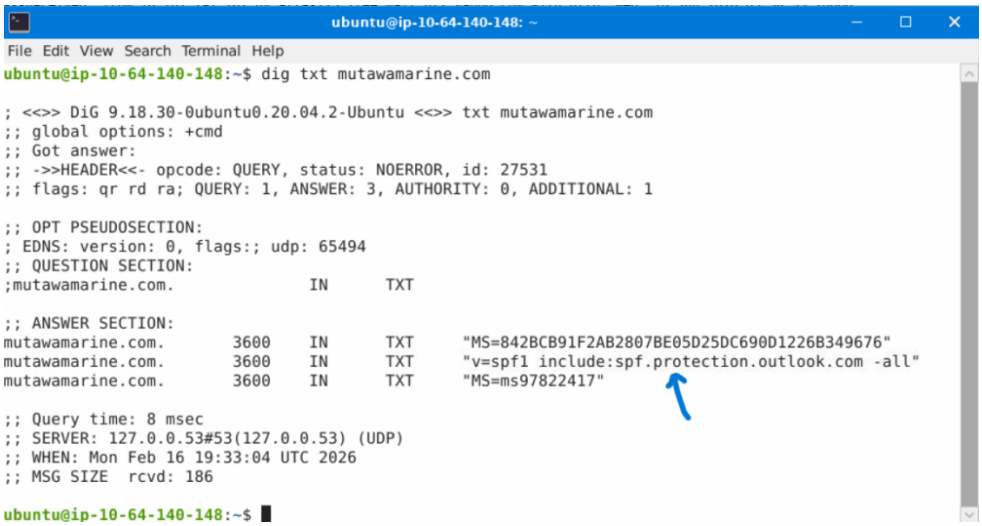
Answer: Hostwinds LLC

What is the SPF record for the Return-Path domain?

Let's analyse another part of our source information.



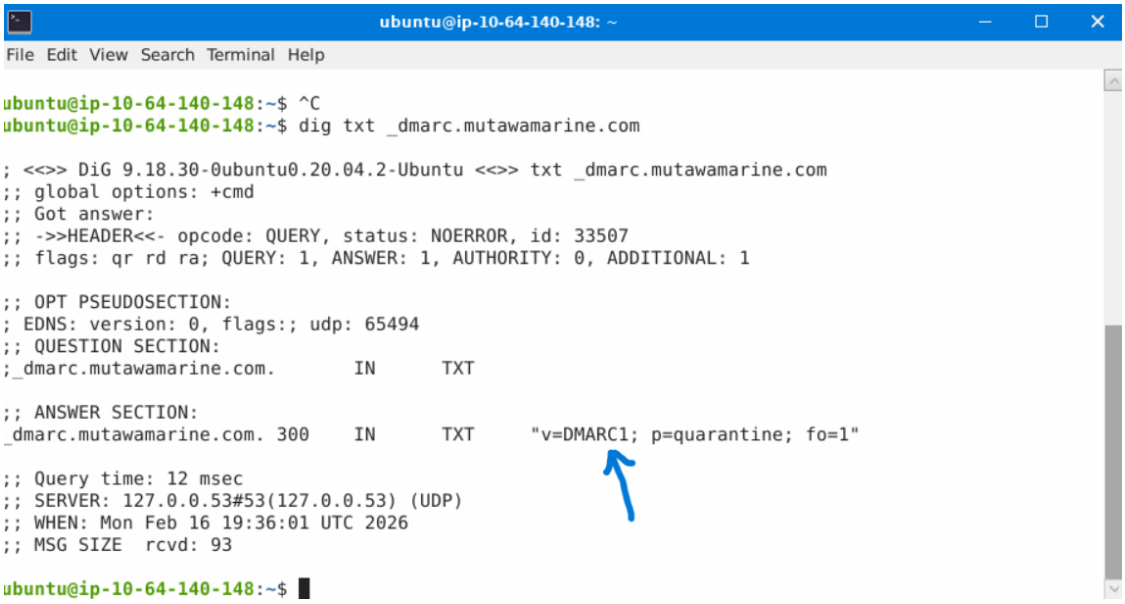
So, we need to check the SPF (Sender Policy Framework) record for mutawamarine.com. It can be done via *dig* (Domain Information Groper) command. This command is used to query DNS nameservers for various domain information. We also use *txt* option to get the TXT records of the domain.



Answer: v=spf1 include:spf.protection.outlook.com -all

What is the DMARC record for the Return-Path domain?

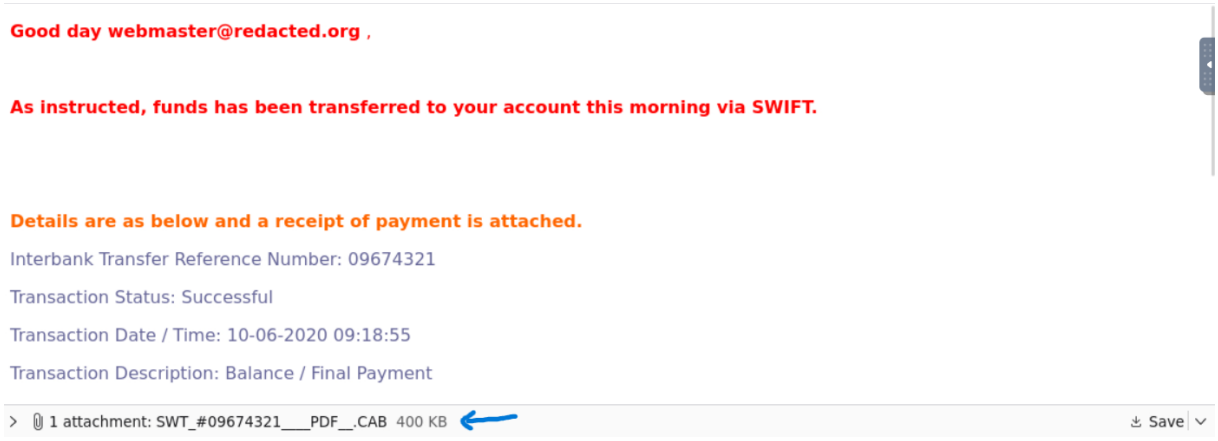
This is done similarly to the previous task. Let's reuse the command and adjust it for DMARC records.



Answer: v=DMARC1; p=quarantine; fo=1

What is the name of the attachment?

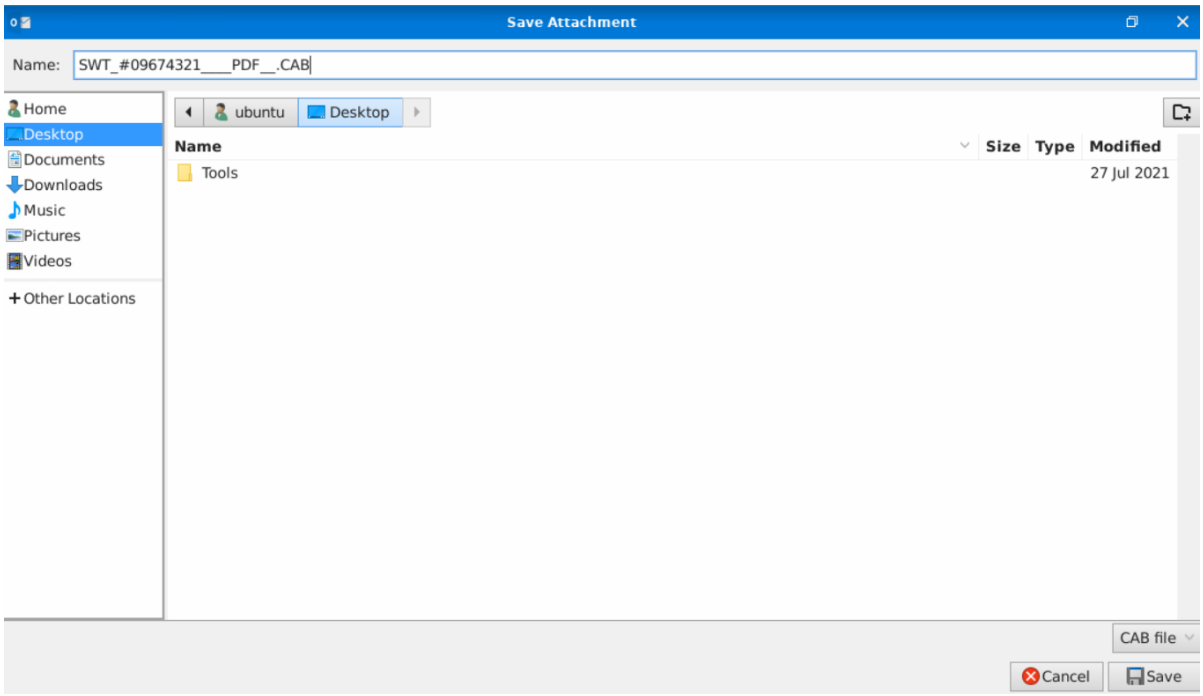
Here all we need to do is to scroll down to the end of the email and find the attachment name.



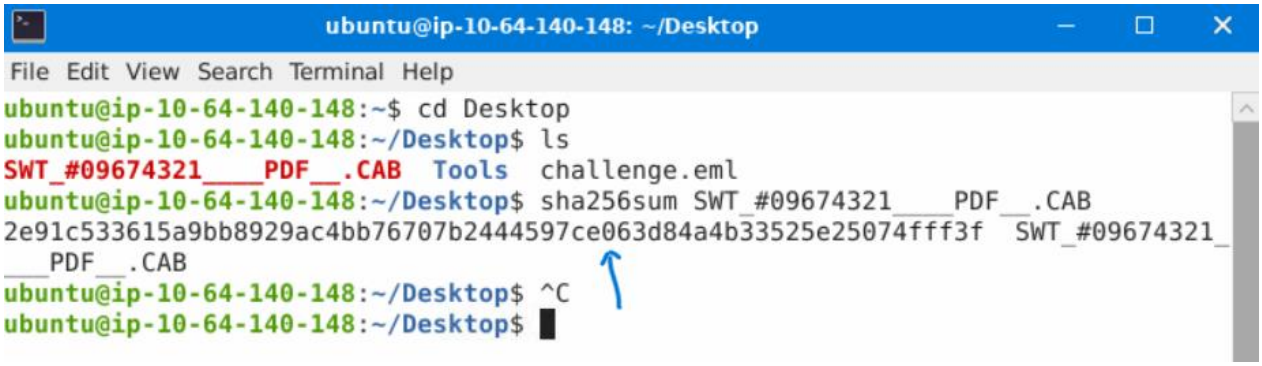
Answer: SWT_#09674321____PDF__.CAB

What is the SHA256 hash of the file attachment?

Let's save this attachment to the VM. It is located in *Desktop*.



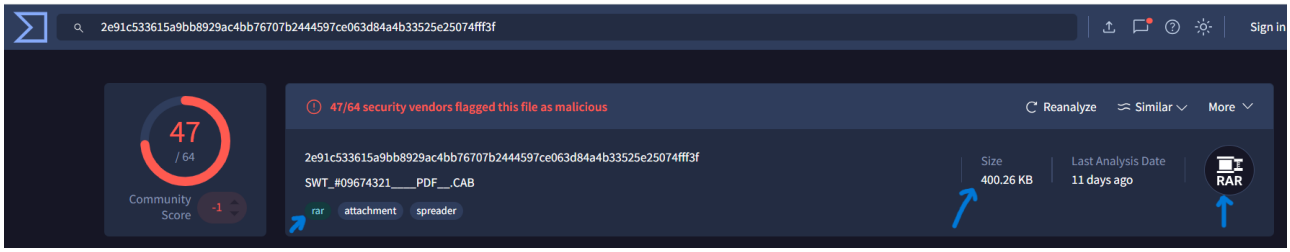
Then we go to the terminal to obtain the hash of this file. We navigate to the Desktop via *cd* command, list the Desktop's content via *ls* and get the hash with the *sha256sum*, which is used to calculate SHA-256 hash values.



Answer:
2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f

What is the attachments file size? What is the actual file extension of the attachment?

Let's check the hash value via VirusTotal. By doing that we solve both these questions.



Answer:

- **400.26 KB**
- **RAR**

Answering the question from Scenario: this is the non-legitimate phishing email.

4. References

- https://www.virustotal.com/gui/home/upload