

The Greenholt Phish – Challenge

2026/01/13

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.

Step 1: What is the **Transfer Reference Number** listed in the email's **Subject**?

From Mr. James Jackson <info@mutawamarine.com> @
To webmaster@redacted.org @ 6/10/20, 05:58
Reply to Mr. James Jackson <info.mutawamarine@mail.com> @
Subject **webmaster@redacted.org your: Transfer Reference Number:(09674321)**

Looking at the Header of the email, I identified the Transfer Reference Number – **09674321**.

Step 2: Who is the email from?

From Mr. James Jackson <info@mutawamarine.com> @
To webmaster@redacted.org @ 6/10/20, 05:58
Reply to Mr. James Jackson <info.mutawamarine@mail.com> @
Subject **webmaster@redacted.org your: Transfer Reference Number:(09674321)**

Working in the same header again, I identified the Sender - **Mr. James Jackson**.

Step 3: What is his email address?

From Mr. James Jackson <info@mutawamarine.com> @
To webmaster@redacted.org @ 6/10/20, 05:58
Reply to Mr. James Jackson <info.mutawamarine@mail.com> @
Subject **webmaster@redacted.org your: Transfer Reference Number:(09674321)**

His email - **info@mutawamarine.com**.

Step 4: What email address will receive a reply to this email?

From Mr. James Jackson <info@mutawamarine.com> @
To webmaster@redacted.org @ 6/10/20, 05:58
Reply to Mr. James Jackson <info.mutawamarine@mail.com> @
Subject **webmaster@redacted.org your: Transfer Reference Number:(09674321)**

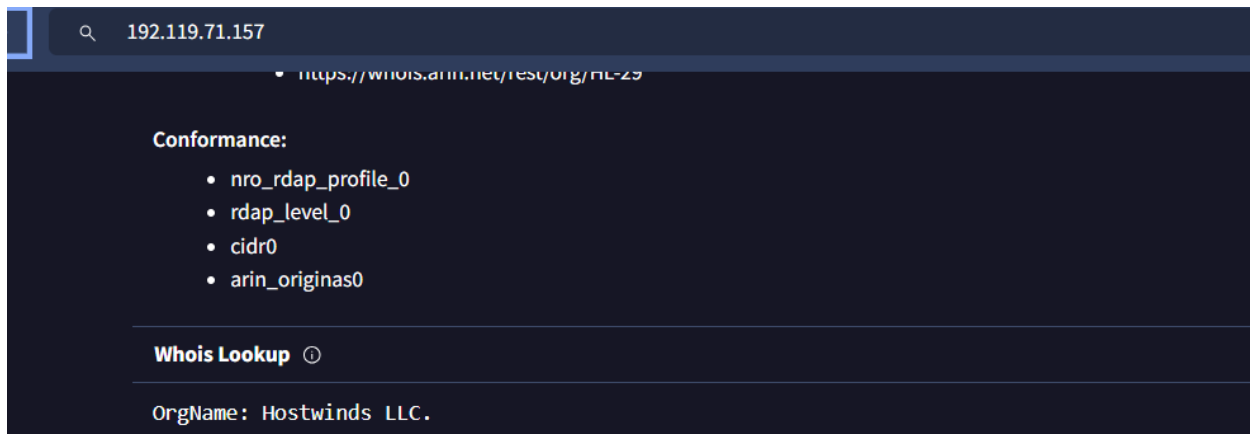
info.mutawamarine@mail.com.

Step 4: What is the Originating IP?

The screenshot shows the Cyberchef web interface. On the left is a sidebar with 'Operations' including defang, Defang URL, Defang IP Addresses, Favourites, Data format, Encryption / Encoding, Public Key, Arithmetic / Logic, and Networking. The main area is divided into 'Input' and 'Output' sections. The 'Input' section shows a file named 'challenge.eml' with a size of 561,873 bytes, type 'message/rfc822', and loaded at 100%. The 'Output' section shows the email header information: 'Jun 2020 05:58:54 +0000', 'Received: from hwsrv-737338.hostwindsdns.com ([192.119.71.157]:51810 helo=mutawamarine.com) by sub.redacted.com with esmtp (Exim 4.80)'. The IP address 192.119.71.157 is highlighted in blue.

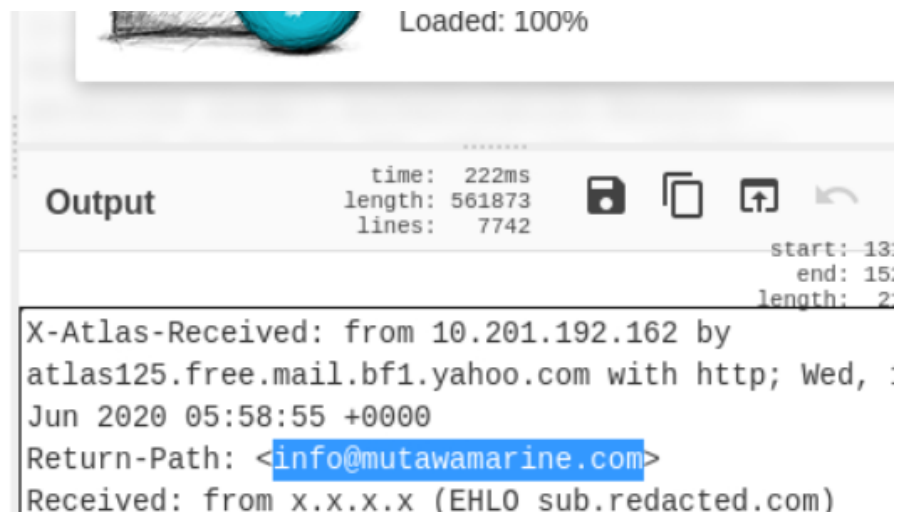
I opened up **Cyberchef** for this one. I brought in the file on Input and In the Output, I managed to identify the Originating IP – **192.119.71.157**.

Step 5: Who is the owner of the Originating IP? (Do not include the "." in your answer.)



For this I copied the IP - **192.119.71.157**. I opened 'VirusTotal' and pasted it there. I clicked on Details and scrolled down to 'Whois Lookup' and found the originating name - **Hostwinds LLC**.

Step 6: What is the SPF record for the Return-Path domain?



I opened up **Cyberchef** and navigated to the Return-Path and found the domain – **mutawarine.com**.

✓ SPF

Great job! You have a valid SPF record, which specifies a hard fail (-all).

— Details

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

To understand and fix the specific errors, use our [SPF Surveyor](#).

I opened up **Dmarcian** and pasted the domain I copied earlier. I then clicked search and scrolled down to SPF and clicked Details to view the record - `v=spf1 include:spf.protection.outlook.com -all`.

Step 7: What is the DMARC record for the Return-Path domain?

ⓘ DMARC

Your domain has a valid DMARC record and it is set to p=quarantine. To fully take advantage of DMARC, the policy should be set to p=reject.

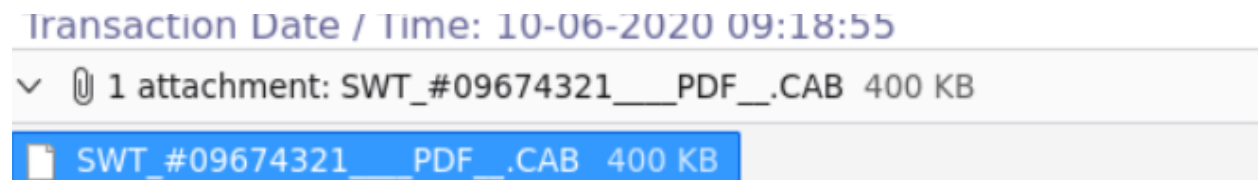
— Details

```
v=DMARC1; p=quarantine; fo=1
```

To understand and fix the specific errors, use our [DMARC Inspector](#).

The DMARC record - `v=DMARC1; p=quarantine; fo=1`.

Step 8: What is the name of the attachment?



I scrolled down to the end of the email and clicked the arrow pointing down – **SWT_#09674321____PDF____.CAB**.

Step 9: What is the SHA256 hash of the file attachment?

```
ubuntu@ip-10-64-138-170:~$ dir
Desktop Documents Downloads Music Pictures Public Templates Videos
ubuntu@ip-10-64-138-170:~$ cd Desktop
ubuntu@ip-10-64-138-170:~/Desktop$ ls
SWT_#09674321__PDF__.CAB  Tools  challenge.eml
ubuntu@ip-10-64-138-170:~/Desktop$ SHA256sum SWT_#09674321__PDF__.CAB
SHA256sum: command not found
ubuntu@ip-10-64-138-170:~/Desktop$ sha256sum SWT_#09674321__PDF__.CAB
2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f  SWT_#09674321__PDF__.CAB
```

I saved the attachment from the email, navigated through the directories and found the hash - **2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f**.

Step 10: What is the attachments file size? (Don't forget to add "KB" to your answer, **NUM KB**)

2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f	
File size	400.26 KB (409868 bytes)

I copied the hash and opened up VirusTotal and pasted it and scrolled down to identify the file size – **400.26 KB**.

Step 11: What is the actual file extension of the attachment?

2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f	
SHA256	2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f
SSDEEP	12288:Mj6ygt8RoYqMAnuL8l0A81aBYolm9+X3B4k56:EgqRJCuL87tolC+X3O
TLSH	T12C94238893562439A8F7385DAFD0CFB5EFE898E74E8F97709CFD609E5D140446205AC2
File type	RAR compressed rar

RAR.

Conclusion Summary

This challenge simulated a real-world SOC phishing investigation and required a structured analysis of a suspicious business email. By examining the email headers, sender and reply-to details, and originating IP address, I was able to identify inconsistencies that indicated the message was not legitimate. Investigating the IP ownership and validating SPF and DMARC records further reinforced how attackers abuse trusted-looking domains and infrastructure to bypass initial scrutiny.

The attachment analysis provided additional confirmation of malicious intent. By identifying the attachment name, calculating its SHA-256 hash, verifying its size through VirusTotal, and uncovering the true file extension hidden behind a misleading filename, I demonstrated safe handling and validation of potentially harmful files.

Overall, this exercise strengthened my ability to correlate email metadata, authentication records, and attachment indicators to confidently assess phishing attempts and produce clear, evidence-based conclusions aligned with real-world SOC investigation practices.