

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.

Good day webmaster@redacted.org .
As instructed, funds has been transferred to your account this morning via SWIFT.

Details are as below and a receipt of payment is attached.

Interbank Transfer Reference Number: 09674321

Transaction Status: Successful

Transaction Date / Time: 10-06-2020 09:18:55

Transaction Description: Balance / Final Payment

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*.

Good day webmaster@redacted.org .
As instructed, funds has been transferred to your account this morning via SWIFT.

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.

```
Source of: file:///home/ubuntu/Desktop/challenge.eml?type=application/x-message-display - Mozilla Thunderbird
File Edit View Help
68ATikwtW3bprt_p1qtpbNPt2wuAsJ1ai/_/Q0_4x3khgYrC4j1mXjV8WDVKV
wTOAdlQ716U8TVp_0AKvevkfMzfzoT0TsGLQ0U.w8uZhv_6mwKB4sW7Pbhbr
B1RJad0va2Cj1CbAC1Onamp5egIEexkhboy810ufz0qkD1al_tn5nv1lx0
bcQer07cnAjpN1amfuvc8gjD345pb6k9l7h7a8Tfsv_67Nrok_.M4_MRZcf
.iuxpcffE2r1ocasfwQ0g6yof0W0ta51sbwQidg7B_4XR2_6cbg8Ui39t2v2Y
bgWIshtBlurfrp_b1SAN7fvE22zvzjz4_4PbBtBDevFUB7pj0GiaE_Nx_
YpW8pLoFasyi1k4T9f5e5ryqau.HToIegVmVa4xwuzjbNvaE7Tsm4m3vepb
zGZ1IBwUDLQ-
X-Originating-IP: [x.x.x.x] 
Received: from 10.197.41.148 (EHLO sub.redacted.com) (x.x.x.x)
  by mta4212.mail.bf1.yahoo.com with SMTP; Wed, 10 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)
  (envelope-from <info@mutawamarine.com>)
  id 1jiss0-0004g5-Ts
  for webmaster@redacted.org; Wed, 10 Jun 2020 01:02:04 -0400
Reply-To: "Mr. James Jackson" <info@mutawamarine@mail.com>
From: "Mr. James Jackson" <info@mutawamarine.com>
To: webmaster@redacted.org
Subject: webmaster@redacted.org your: Transfer Reference Number:(09674321)
Date: 09 Jun 2020 22:58:27 -0700
Message-ID: <20200609225823.DFAEAAF31A6B7414@mutawamarine.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
  boundary="----=_NextPart_000_0012_BDB07B06.81B59493"
X-Spam-Status: No, score=-0.5
X-Spam-Score: -4
X-Spam-Bar: /
X-Ham-Report: Spam detection software, running on the system "sub.redacted.com", has
  identified this incoming email as possible spam. The original message
  has been attached to this so you can view it (if it isn't spam) or label
  similar future email. If you have any questions, see
  the administrator of that system for details.
```

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.

```
Source of: file:///home/ubuntu/Desktop/challenge.eml?type=application/x-message-display - Mozilla Thunderbird
File Edit View Help
68ATikwtW3bprt_p1qtpbNPt2wuAsJ1ai/_/Q0_4x3khgYrC4j1mXjV8WDVKV
wTOAdlQ716U8TVp_0AKvevkfMzfzoT0TsGLQ0U.w8uZhv_6mwKB4sW7Pbhbr
B1RJad0va2Cj1CbAC1Onamp5egIEexkhboy810ufz0qkD1al_tn5nv1lx0
bcQer07cnAjpN1amfuvc8gjD345pb6k9l7h7a8Tfsv_67Nrok_.M4_MRZcf
.iuxpcffE2r1ocasfwQ0g6yof0W0ta51sbwQidg7B_4XR2_6cbg8Ui39t2v2Y
bgWIshtBlurfrp_b1SAN7fvE22zvzjz4_4PbBtBDevFUB7pj0GiaE_Nx_
YpW8pLoFasyi1k4T9f5e5ryqau.HToIegVmVa4xwuzjbNvaE7Tsm4m3vepb
zGZ1IBwUDLQ-
X-Originating-IP: [x.x.x.x]
Received: from 10.197.41.148 (EHLO sub.redacted.com) (x.x.x.x)
  by mta4212.mail.bf1.yahoo.com with SMTP; Wed, 10 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)
  (envelope-from <info@mutawamarine.com>)
  id 1jiss0-0004g5-Ts
  for webmaster@redacted.org; Wed, 10 Jun 2020 01:02:04 -0400
Reply-To: "Mr. James Jackson" <info@mutawamarine@mail.com>
From: "Mr. James Jackson" <info@mutawamarine.com>
To: webmaster@redacted.org
Subject: webmaster@redacted.org your: Transfer Reference Number:(09674321)
Date: 09 Jun 2020 22:58:27 -0700
Message-ID: <20200609225823.DFAEAAF31A6B7414@mutawamarine.com>
MIME-Version: 1.0
Content-Type: multipart/mixed;
  boundary="----=_NextPart_000_0012_BDB07B06.81B59493"
X-Spam-Status: No, score=-0.5
X-Spam-Score: -4
X-Spam-Bar: /
X-Ham-Report: Spam detection software, running on the system "sub.redacted.com", has
  identified this incoming email as possible spam. The original message
  has been attached to this so you can view it (if it isn't spam) or label
  similar future email. If you have any questions, see
  the administrator of that system for details.
```

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.

```
Source of: file:///home/ubuntu/Desktop/challenge.eml?type=application/x-message-display - Mozilla Thunderbird
File Edit View Help
X-Atlas-Received: from 10.201.192.162 by atlas125.free.mail.bf1.yahoo.com with http; Wed, 10 Jun 2020 05:58:55 +0000
Return-Path: <info@mutawamarine.com>
Received: from x.x.x.x (EHLO sub.redacted.com)
by atlas125.free.mail.bf1.yahoo.com with SMTPs; Wed, 10 Jun 2020 05:58:55 +0000
X-Originating-Ip: [x.x.x.x]
Received-SPF: fail (domain of mutawamarine.com does not designate x.x.x.x as permitted sender)
Authentication-Results: atlas125.free.mail.bf1.yahoo.com;
spf=fail smtp.mailfrom=mutawamarine.com;
dmarc=unknown
```

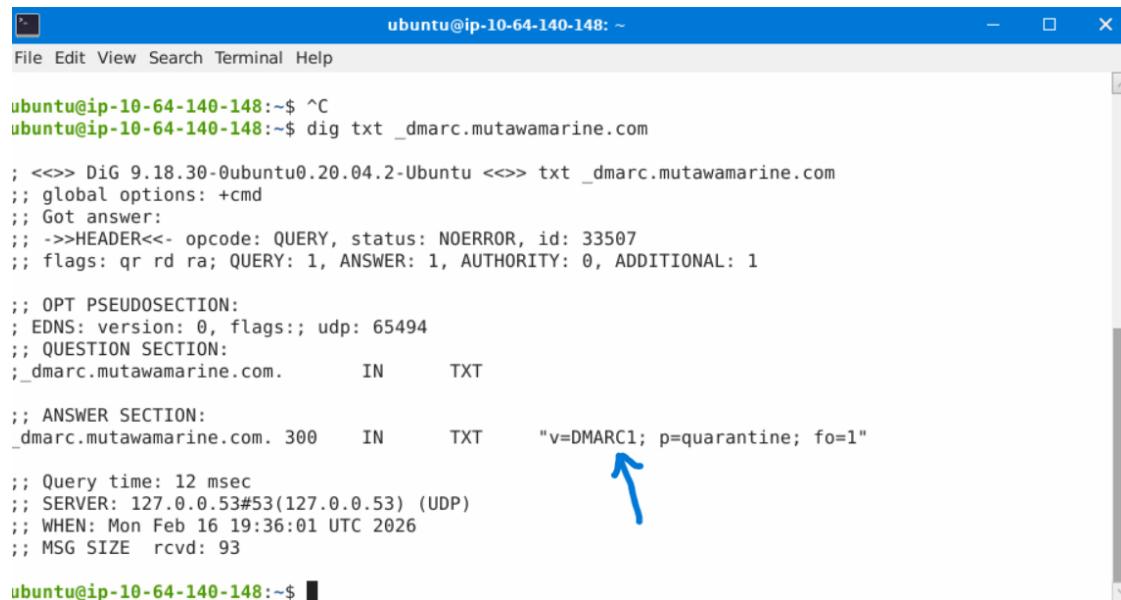
So, we need to check the SPF (Sender Policy Framework) record for mutawamarine.com. It can be done via *dig* (Domain Information Groper) command. This command is used to query DNS nameservers for various domain information. We also use *txt* option to get the TXT records of the domain.

```
ubuntu@ip-10-64-140-148:~$ dig txt mutawamarine.com
; <>> DiG 9.18.30-0ubuntu0.20.04.2-Ubuntu <>> txt mutawamarine.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 27531
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: udp: 65494
;; QUESTION SECTION:
;mutawamarine.com.      IN      TXT
;; ANSWER SECTION:
mutawamarine.com. 3600   IN      TXT    "MS=842BCB91F2AB2807BE05D25DC690D1226B349676"
mutawamarine.com. 3600   IN      TXT    "v=spf1 include:spf.protection.outlook.com -all"
mutawamarine.com. 3600   IN      TXT    "MS=ms97822417"
;; Query time: 8 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Feb 16 19:33:04 UTC 2026
;; MSG SIZE  rcvd: 186
ubuntu@ip-10-64-140-148:~$
```

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.



```
ubuntu@ip-10-64-140-148:~$ ^C
ubuntu@ip-10-64-140-148:~$ dig txt _dmarc.mutawamarine.com

; <>> DiG 9.18.30-0ubuntu0.20.04.2-Ubuntu <>> txt _dmarc.mutawamarine.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33507
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;_dmarc.mutawamarine.com.      IN      TXT

;; ANSWER SECTION:
_dmarc.mutawamarine.com. 300     IN      TXT      "v=DMARC1; p=quarantine; fo=1"

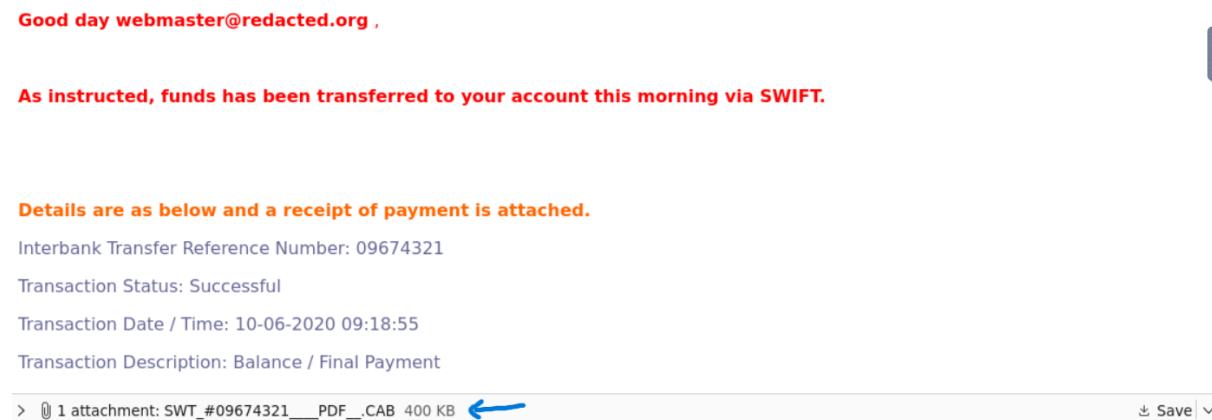
;; Query time: 12 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Mon Feb 16 19:36:01 UTC 2026
;; MSG SIZE rcvd: 93

ubuntu@ip-10-64-140-148:~$
```

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.



Good day webmaster@redacted.org ,

As instructed, funds has been transferred to your account this morning via SWIFT.

Details are as below and a receipt of payment is attached.

Interbank Transfer Reference Number: 09674321

Transaction Status: Successful

Transaction Date / Time: 10-06-2020 09:18:55

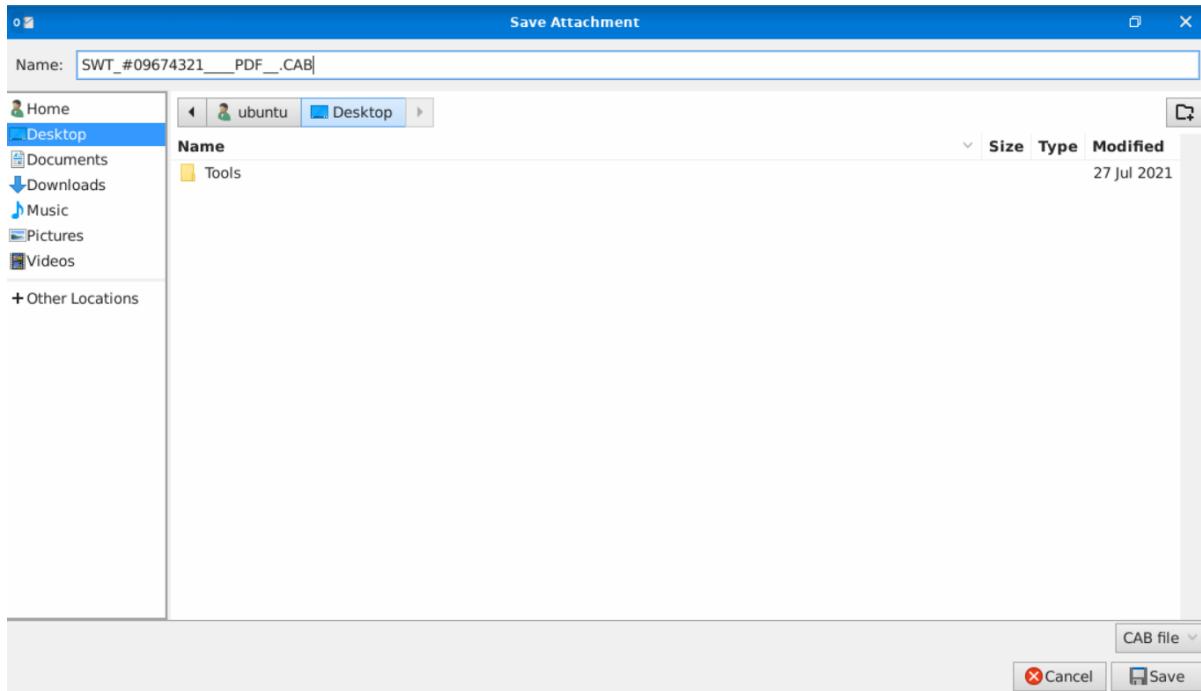
Transaction Description: Balance / Final Payment

> 1 attachment: SWT_#09674321____PDF__.CAB 400 KB

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.

```
ubuntu@ip-10-64-140-148:~/Desktop
File Edit View Search Terminal Help
ubuntu@ip-10-64-140-148:~$ cd Desktop
ubuntu@ip-10-64-140-148:~/Desktop$ ls
SWT_#09674321__PDF__.CAB  Tools  challenge.eml
ubuntu@ip-10-64-140-148:~/Desktop$ sha256sum SWT_#09674321__PDF__.CAB
2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f  SWT_#09674321_
_PDF__.CAB
ubuntu@ip-10-64-140-148:~/Desktop$ ^C
ubuntu@ip-10-64-140-148:~/Desktop$
```

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.

Community Score: 47 / 64

47/64 security vendors flagged this file as malicious

2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f
SWT_#09674321__PDF__.CAB

Size: 400.26 KB | Last Analysis Date: 11 days ago | RAR

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>