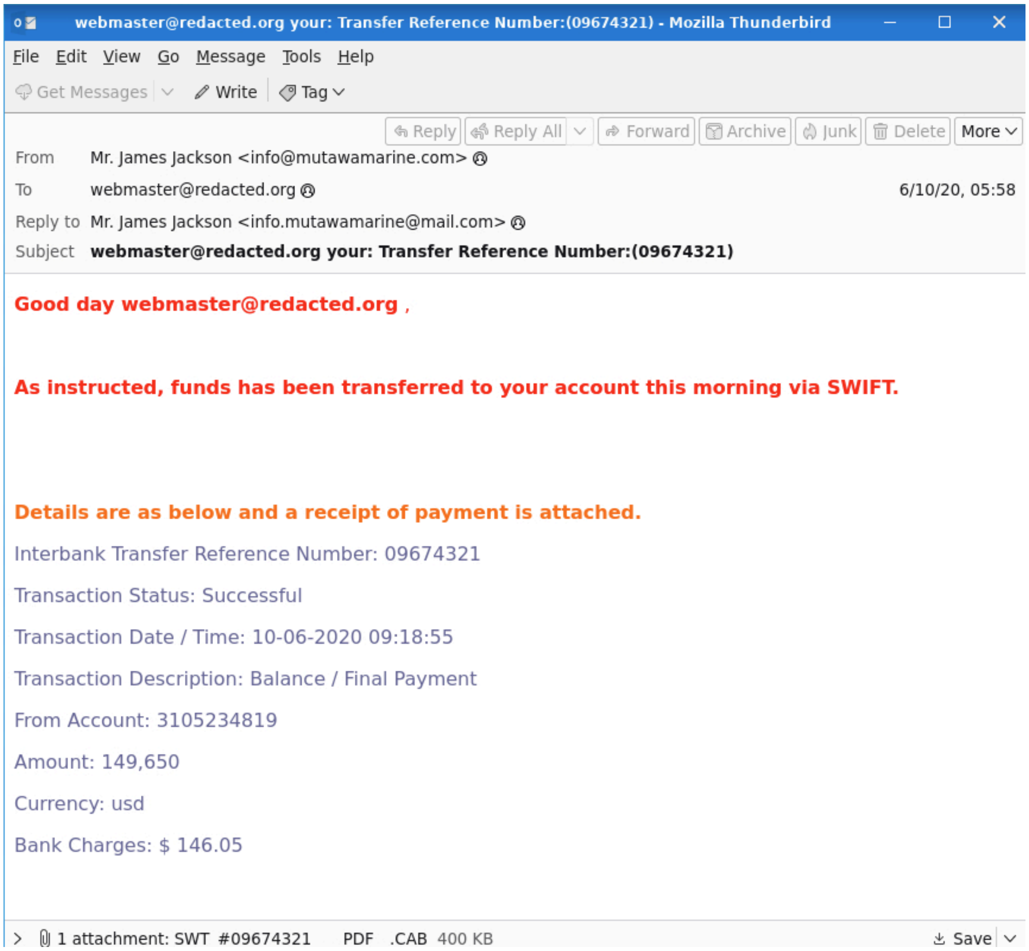
The Greenholt Phish

Created by Alexander Egerev

NOTE: This story was created by me, not by Artificial Intelligence (AI).

The first paragraph was taken from the Greenholt Phish TryHackMe lab. The rest of the story is made up by me as a way of showing what would actually happen in a cybersecurity organization.

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.


webmaster@redacted.org your: Transfer Reference Number:(09674321) - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More

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)**

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

From Account: 3105234819

Amount: 149,650

Currency: usd

Bank Charges: $ 146.05

1 attachment: SWT #09674321 PDF .CAB 400 KB

Save

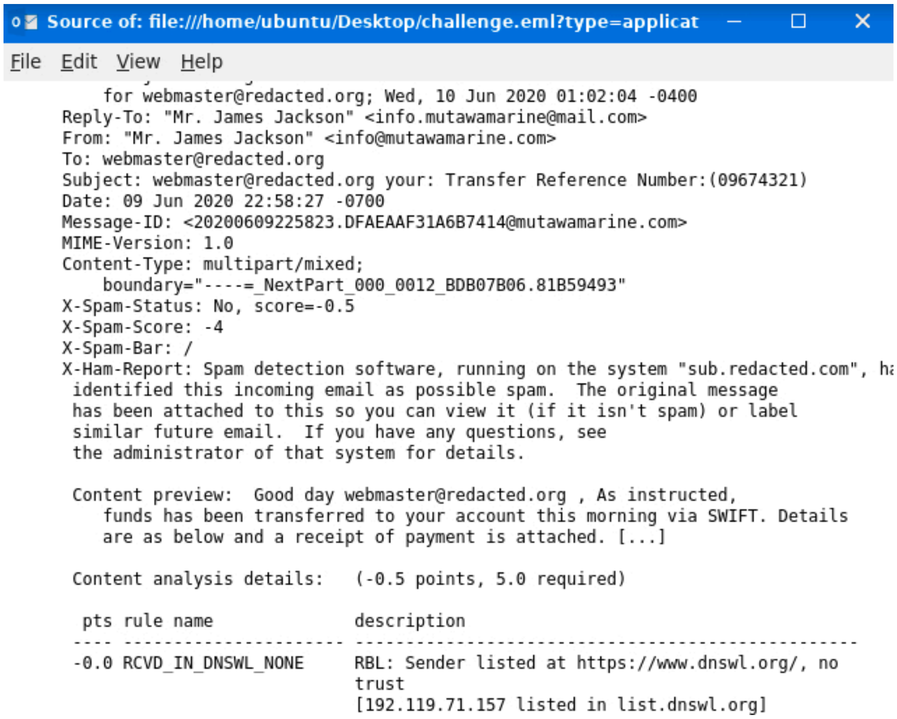
The Security Operations Center department managed to take a close look at the email. Based on this, the team got the following results:

- The email came from Mr. James Jackson from the Mutawa Marine Works.
- The Reply-To section showed the same person (Mr. James Jackson), **but a different email** - info.mutawamarine@mail.com.
- The text body showed the following:
    - "Good day ________" - a generic greeting used by hackers
    - "Details are **as** below", not "Details are below"; 'usd' not 'USD', '149,650' instead of '$149,650' - grammatical errors used by hackers showcasing that whoever wrote this was rushing things. That, or it could be a hacker.
- At the end of the document was an attachment with a .CAB extension. The SOC team forwarded the email with the attachment to the Digital Forensics team, hoping that they could analyze the problem with the attachment.

While the SOC department was waiting for the investigation results from the Digital Forensics team, they were looking at the email, not the attachment. Based on the details of the email, the Originating IP address was 192.119.71.157 - an IP address that looked legitimate. However, after running the IP address through an IP lookup tool, it was confirmed to be hosted by Hostwinds LLC, a hosting company. Analysis of the company proved to be a challenge because the company was NOT real and therefore deemed illegitimate.

The screenshots of the log(s) are shown below:

Source of Email


Source of: file:///home/ubuntu/Desktop/challenge.eml?type=applicat
File
Edit
View
Help

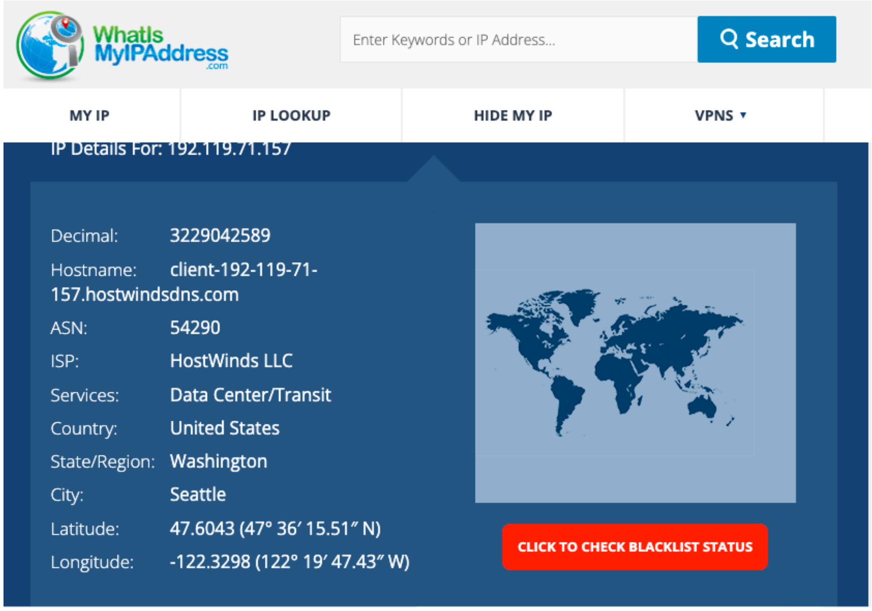
```
    for webmaster@redacted.org; Wed, 10 Jun 2020 01:02:04 -0400
Reply-To: "Mr. James Jackson" <info.mutawamarine@mail.com>
From: "Mr. James Jackson" <info@mutawamarine.com>
To: webmaster@redacted.org
Subject: webmaster@redacted.org your: Transfer Reference Number:(09674321)
Date: 09 Jun 2020 22:58:27 -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", ha
 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.

 Content preview:  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. [...]

 Content analysis details:   (-0.5 points, 5.0 required)

  pts rule name              description
 ---- ---------------------- --------------------------------------------------
 -0.0 RCVD_IN_DNSWL_NONE     RBL: Sender listed at https://www.dnswl.org/, no
                             trust
                             [192.119.71.157 listed in list.dnswl.org]
```

IP Lookup Tool


WhatIs MyIPAddress .com
Enter Keywords or IP Address...
Search
MY IP
IP LOOKUP
HIDE MY IP
VPNS ▾
CLICK TO CHECK BLACKLIST STATUS

IP Details For: 192.119.71.157

Decimal: 3229042589

Hostname: client-192-119-71-157.hostwindsdns.com

ASN: 54290

ISP: HostWinds LLC

Services: Data Center/Transit

Country: United States

State/Region: Washington

City: Seattle

Latitude: 47.6043 (47° 36′ 15.51″ N)

Longitude: -122.3298 (122° 19′ 47.43″ W)

Based on the Lookup Tool, we can see that the hostname is ‘client-192-119-71-157.hostwindsdns.com’ - a common name for a place where hackers can host their malicious sites.

Meanwhile, the Digital Forensics team concluded its investigation of the attachment. Based on their findings, the attachment - which had the .CAB extension (which is often used for software installation, driver installation, and system file packaging) - was really a .rar attachment that, while legitimate, may have contained malware or phishing content.

After careful analysis of the email and the attachment, the Security Operation Center team and the Digital Forensics team came to one simple conclusion: **the email that was sent was indeed a phishing email.** The reasoning above proves it to be true - the 'Reply-To' email being different from the real email, the generic greeting, and the grammatical errors tell it all. Moreover, the .rar attachment proved that the email was a **phishing** email. Additionally, the logs and the IP lookup tools told the story to the team.

As for the type of phishing email, it was an **impersonation** - it came from Mr. James Jackson, who is a customer at Greenholt; however, the sales executive who received it knew that the company's customers never use generic greetings or initiate money transfers.

Once the company found out that it was an impersonation phishing scam, they sent a support ticket directly to the IT Support staff, who alerted the users about it. In the end, nothing was damaged or destroyed.

After the shake-up, the employees were told that they had to complete an online training course in order to be fully aware of those types of emails. They were also told to remember one quote: **If you see something, say something.**