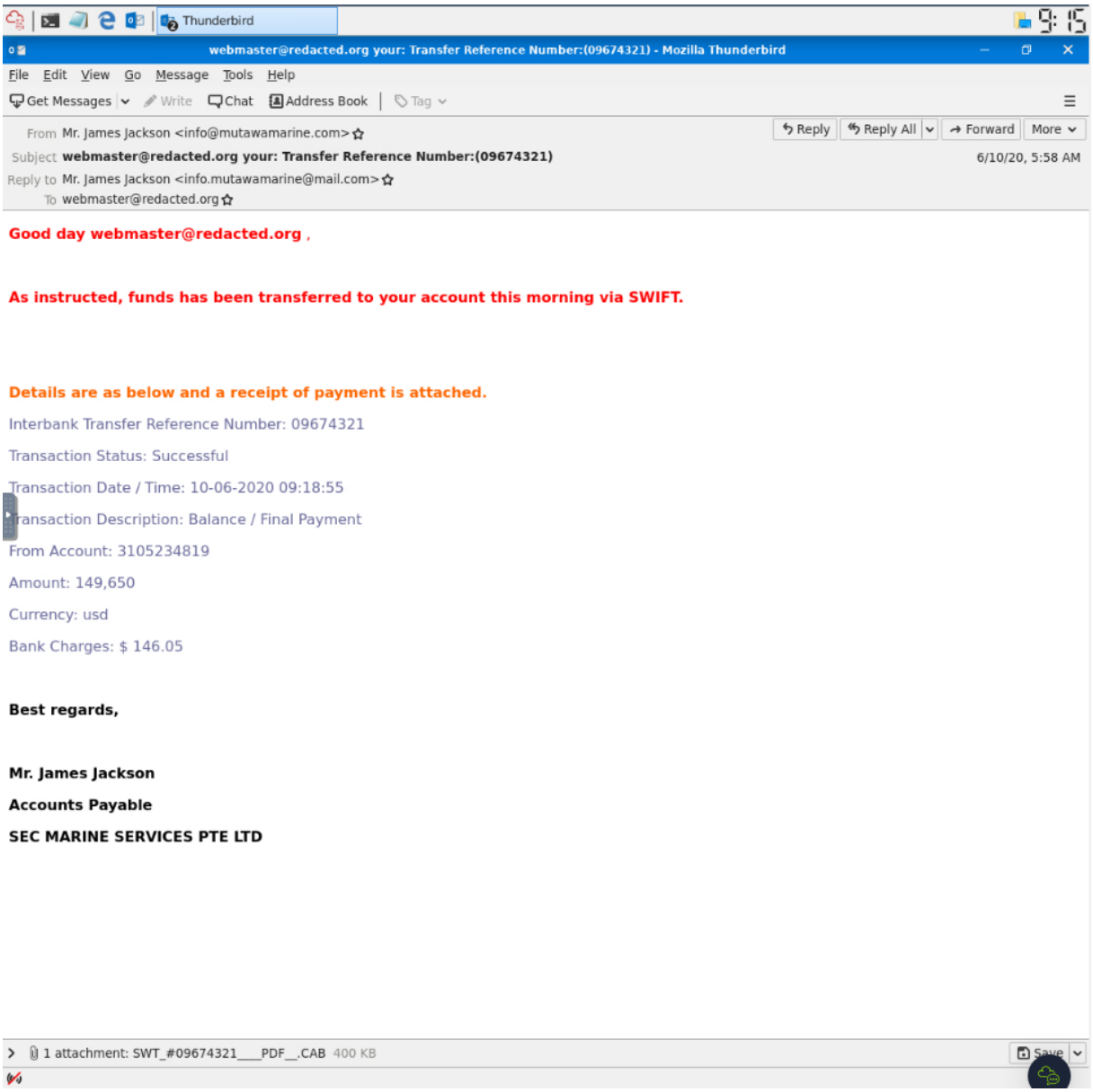
”GreenHolt phish” Phishing Report

Email Description and Artifacts Collected



Sending Address: info@mutawamarine.com
Subject Line: webmaster@redacted.org your: Transfer Reference Number:(09674321)

Recipients: webmaster@redacted.org

Sending Server IP: 192.119.71.157
Reverse DNS: hwsrv-737338.hostwindsdns.com

Reply-To: info.mutawamarine@mail.com
Date and Time: 06/10/2020 05:58

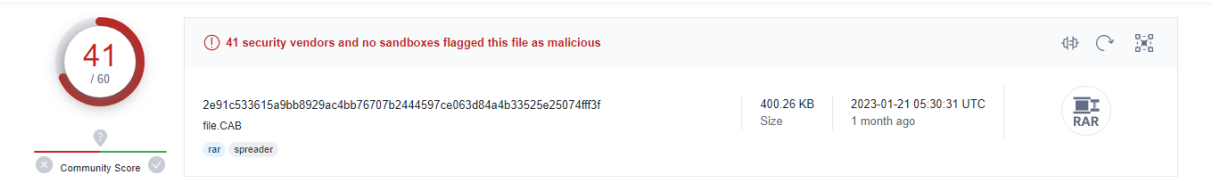
Attachment Name: SWT_#09674321____PDF__.CAB
Attachment SHA256 Hash:
2e91c533615a9bb8929ac4bb76707b2444597ce063d84a4b33525e25074fff3f

Looking at the reported email in the Thunderbird email client, this message is impersonating Mutawa marine, informing recipient that funds have been transferred to their account and trying to get the recipient to open the attached file.

Artifact Analysis

A reverse DNS search on the sending server IP shows that this email originated from Hostwinds LLC infrastructure and not Mutawa marine. The Reply-to line also shows that email did not originate from a Mutawa marine mail address but a @mail.com address.

A VirusTotal search of the attachment shows that the attachment is most likely a malicious Trojan as 41/60 vendors are flagging it as malicious.



Suggested Defensive Measures

The most appropriate action would be to block the specific mailbox to prevent any more incoming malicious emails from this sender, blocking the whole domain would be too much as there could be legitimate emails originating from the @mail.com domain.

The second most appropriate action would be to block the specific attachment hash.