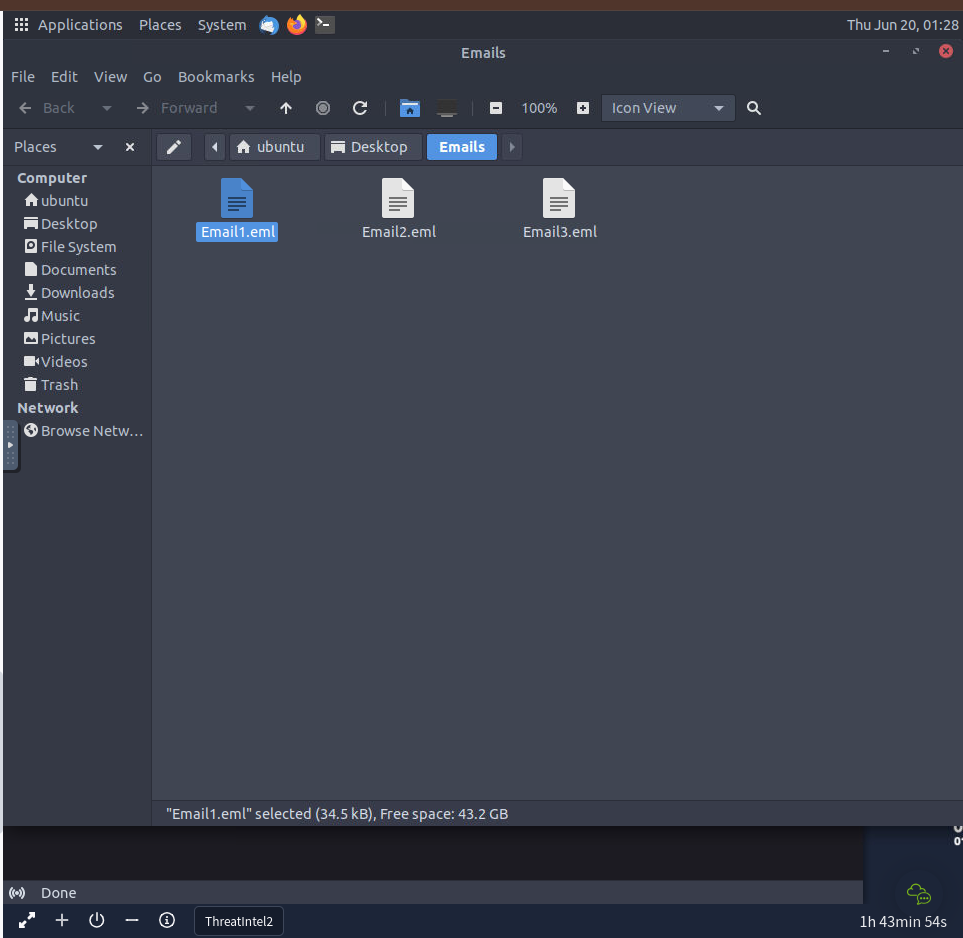
**Email Analysis**

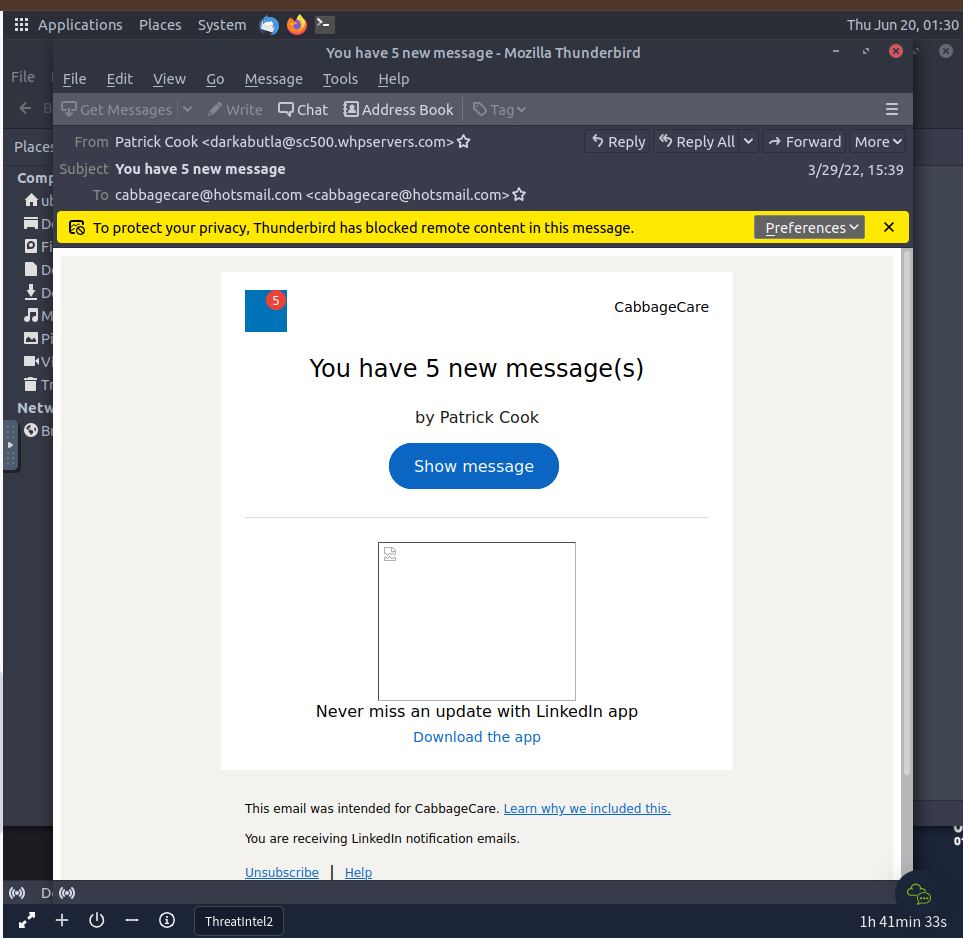
Analyzing an email using Mozilla ThunderBird

We’ll use a sample mail from THM’s Threat Intelligence Tools room.

1. Open the email.



ThunderBird is already installed. The email is then opened.



1. Take in the details

Let’s see who sent us the email. The receiving email address is cabbagecare@hotsmail.com.

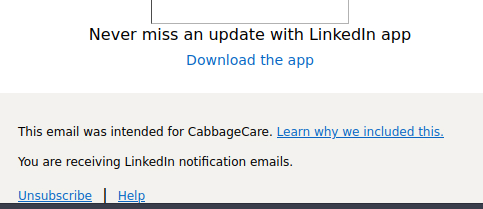


The sender’s mail is [darkabutla@sc500.whpservers.com](mailto:darkabutla@sc500.whpservers.com).



From the address alone, we can have reasonable suspicion that the email is likely spam or malicious.

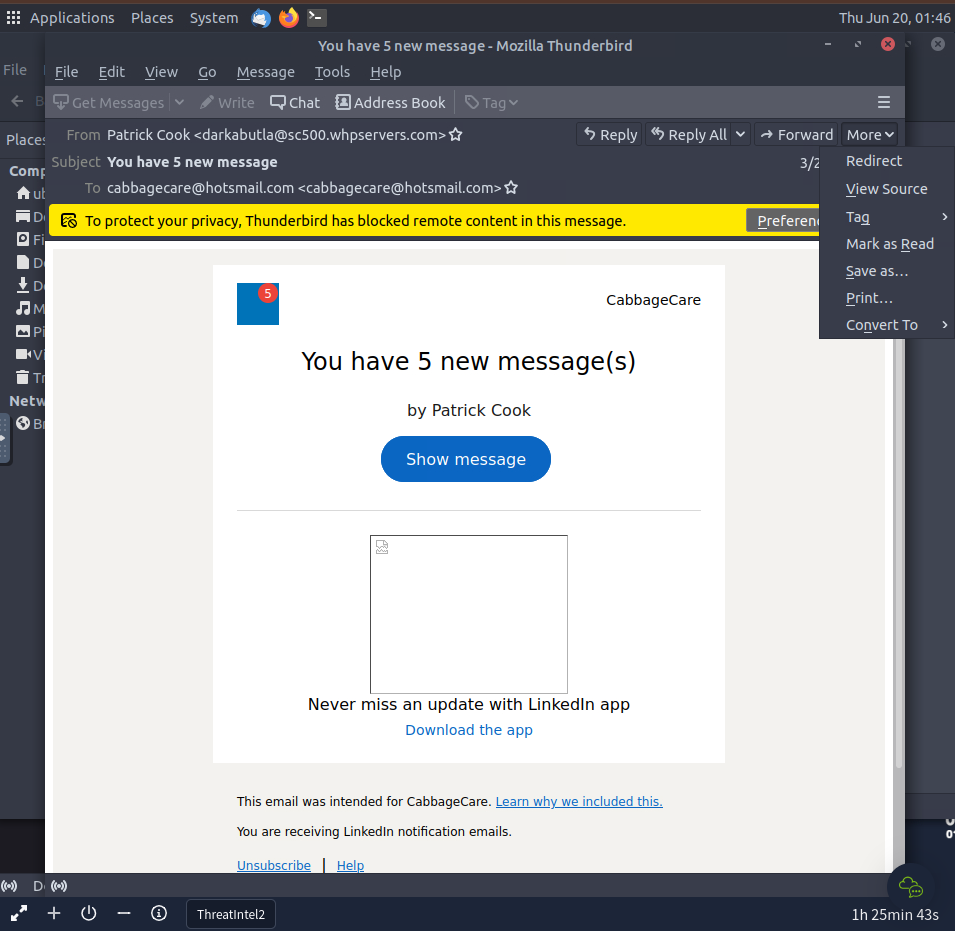
Another thing we can see is that the email claims to be from LinkedIn. It clearly claims “You are receiving LinkedIn notification emails.”



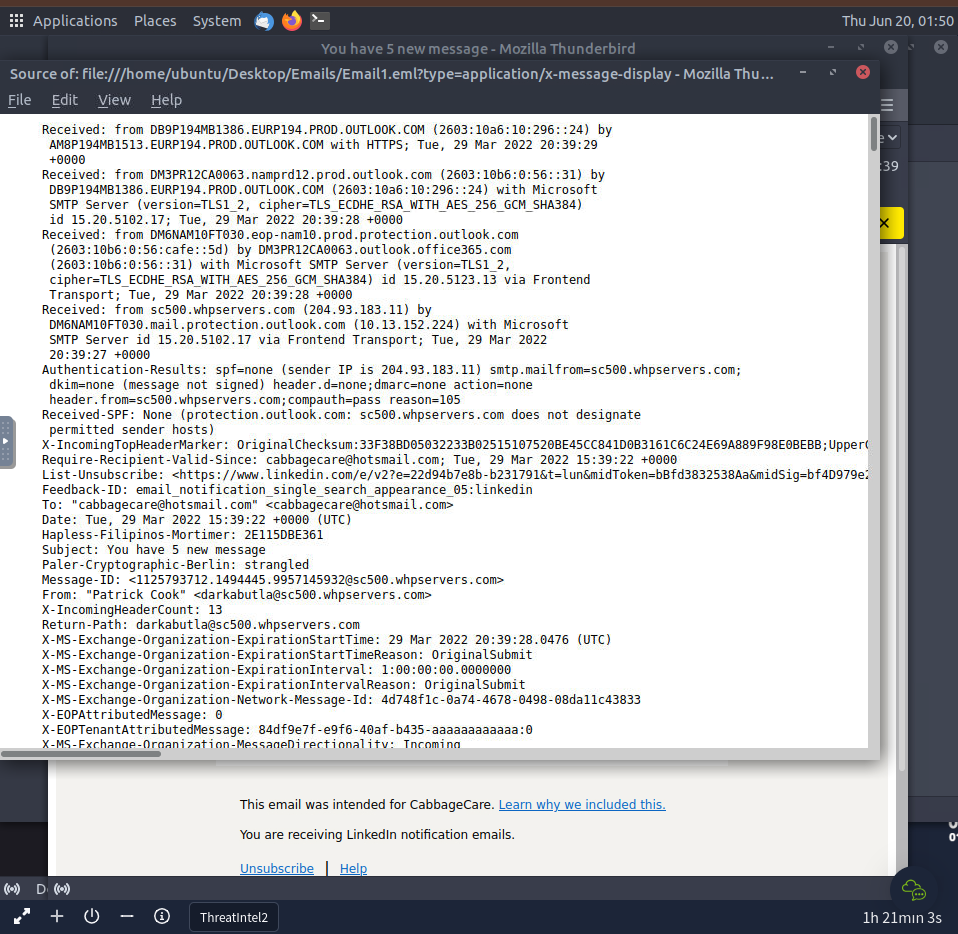
Now we can be sure it is a malicious email. The email address used is not LinkedIn’s address.

1. Mitigation

Let’s get its IP to block it in the firewall settings.



We will view the source.

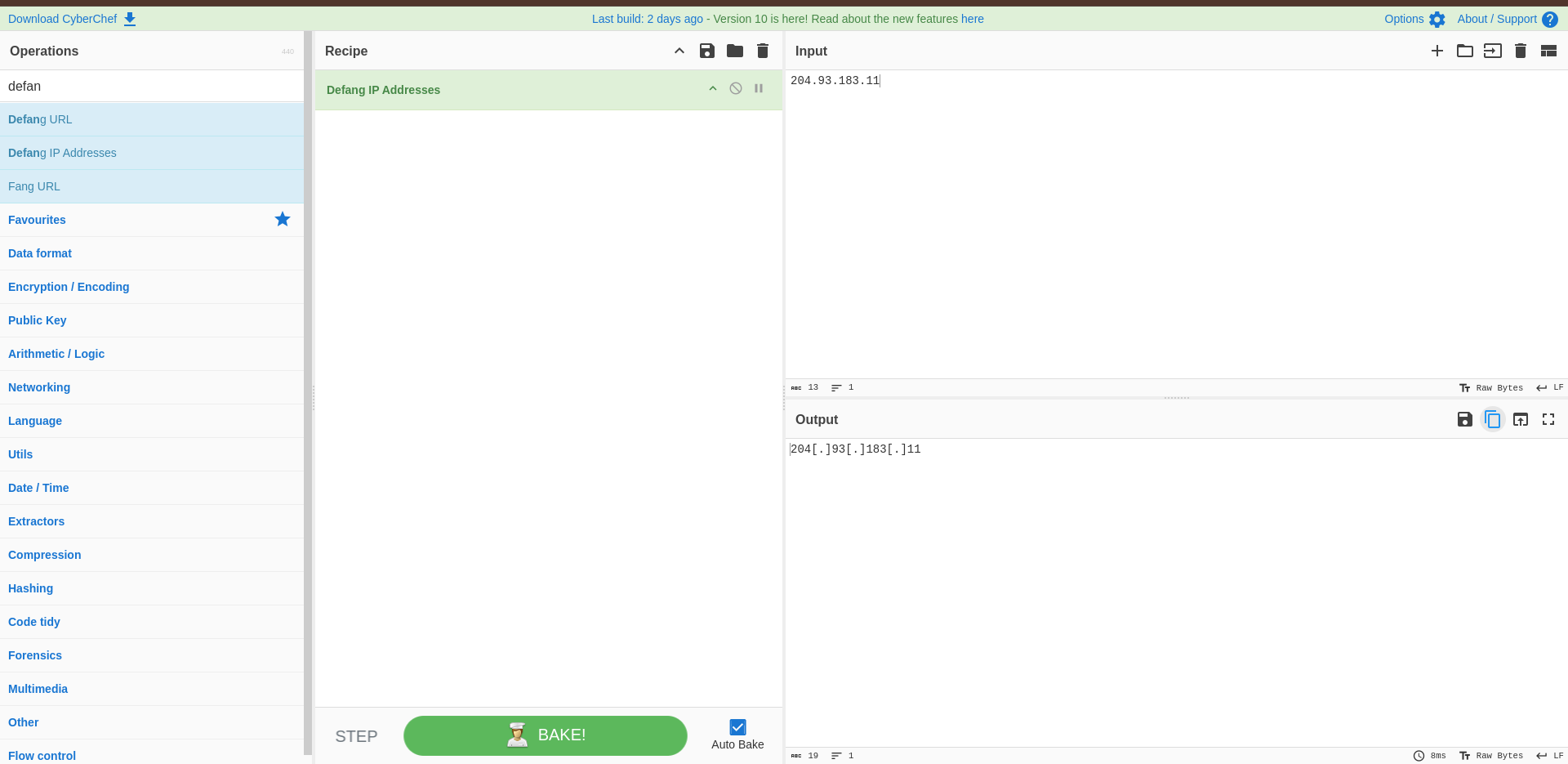


We get the sender’s IP to be 204.93.183.11.

Now to defang it.

There’s a tool called [CyberChef](https://gchq.github.io/CyberChef/) we can use for that.

Once there, search for ‘defang IP’ and then input the sender’s IP to be defanged.



And that’s it!

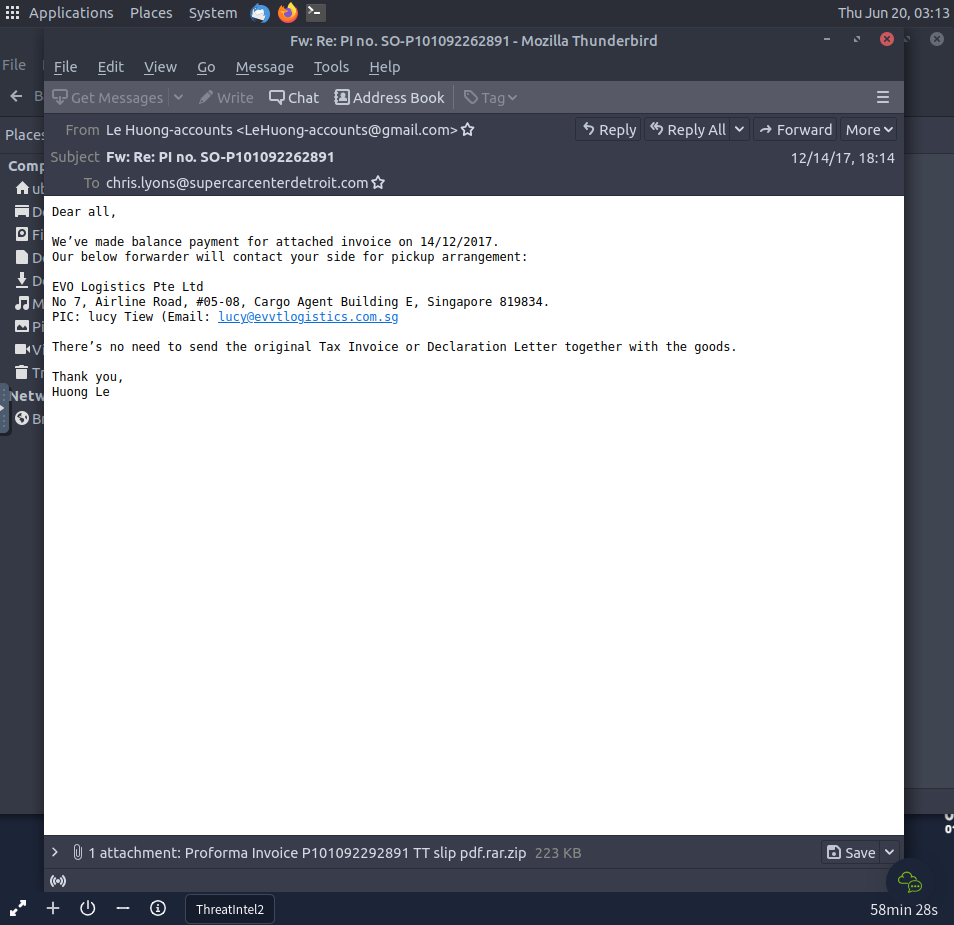
1. What’s next?

Phishing is a common tactic used for cyber attacks. The best way to mitigate the risks associated with it in the long run is to make people aware.

Security awareness programs and practice drills will save a lot of time and potential loss due to data breaches.

Analyzing with Cisco Talos

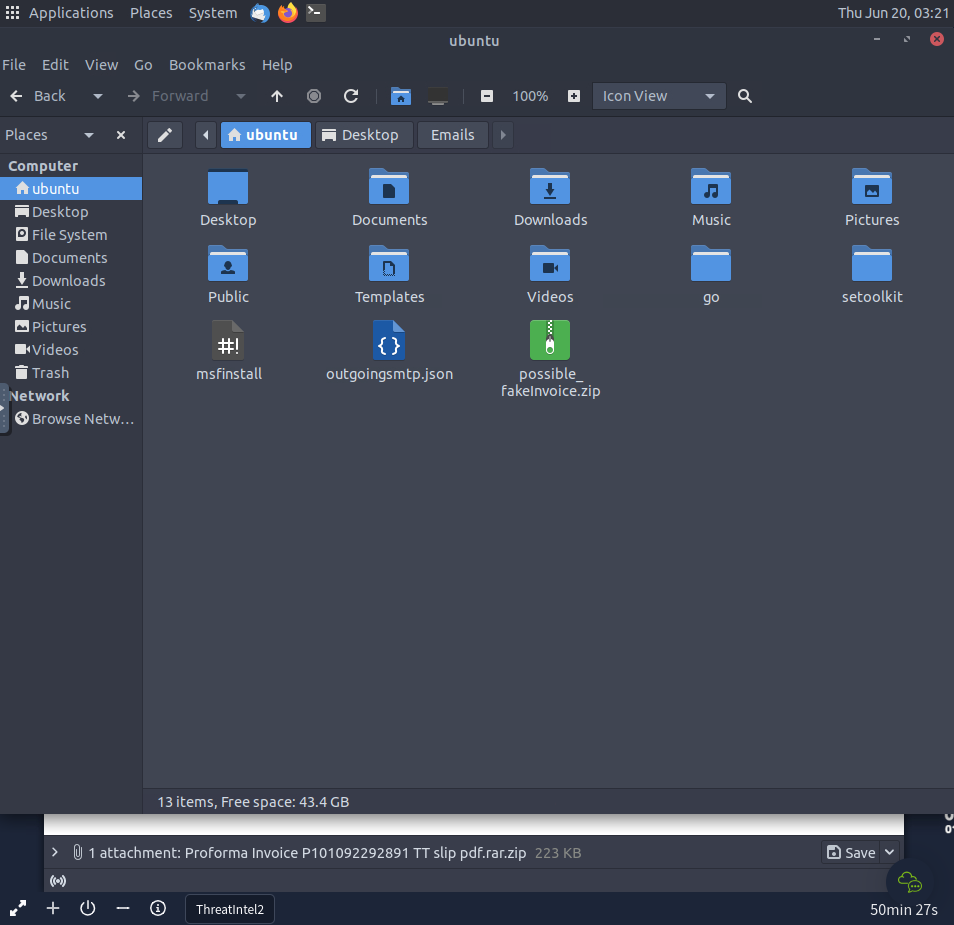
Another email was received claiming to be from an employee at a company, possibly from the customer care department or finance department.



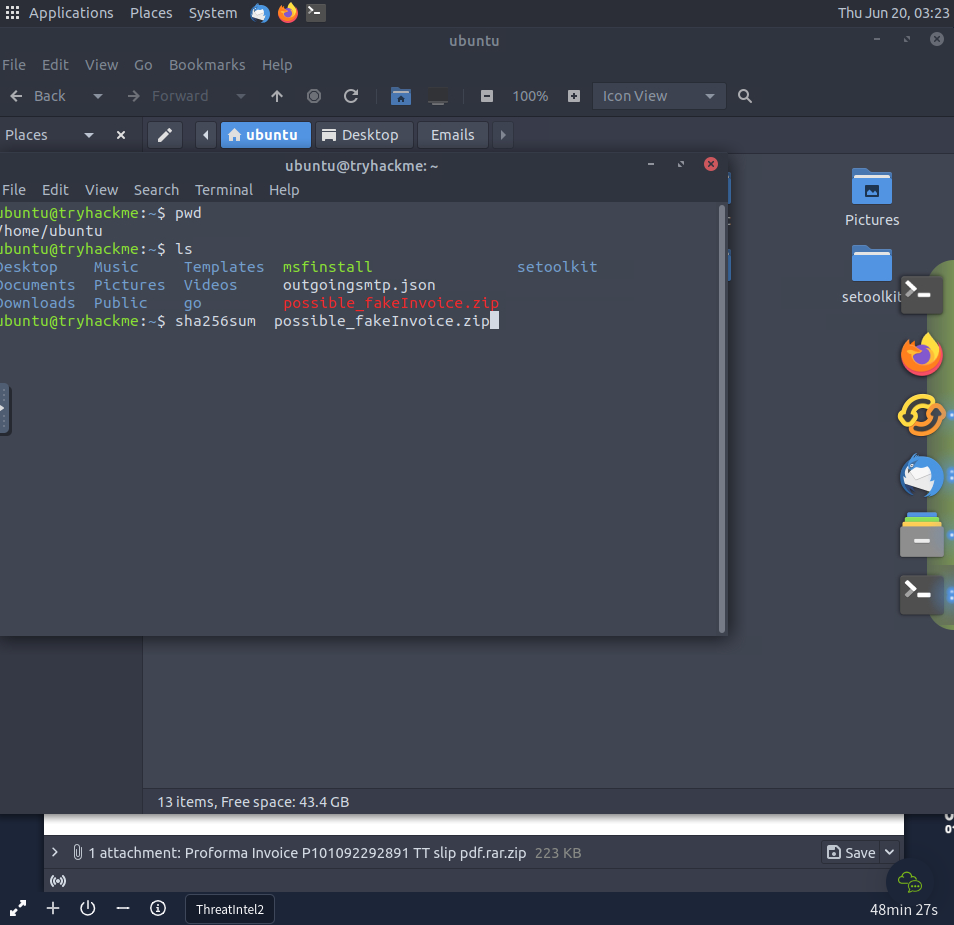
There is a file attachment. Taking in the details, we see that the sender’s email is a personal email. Companies don’t usually use personal emails. It’s possible for small businesses to do so, however, the file attachment raises more suspicion.

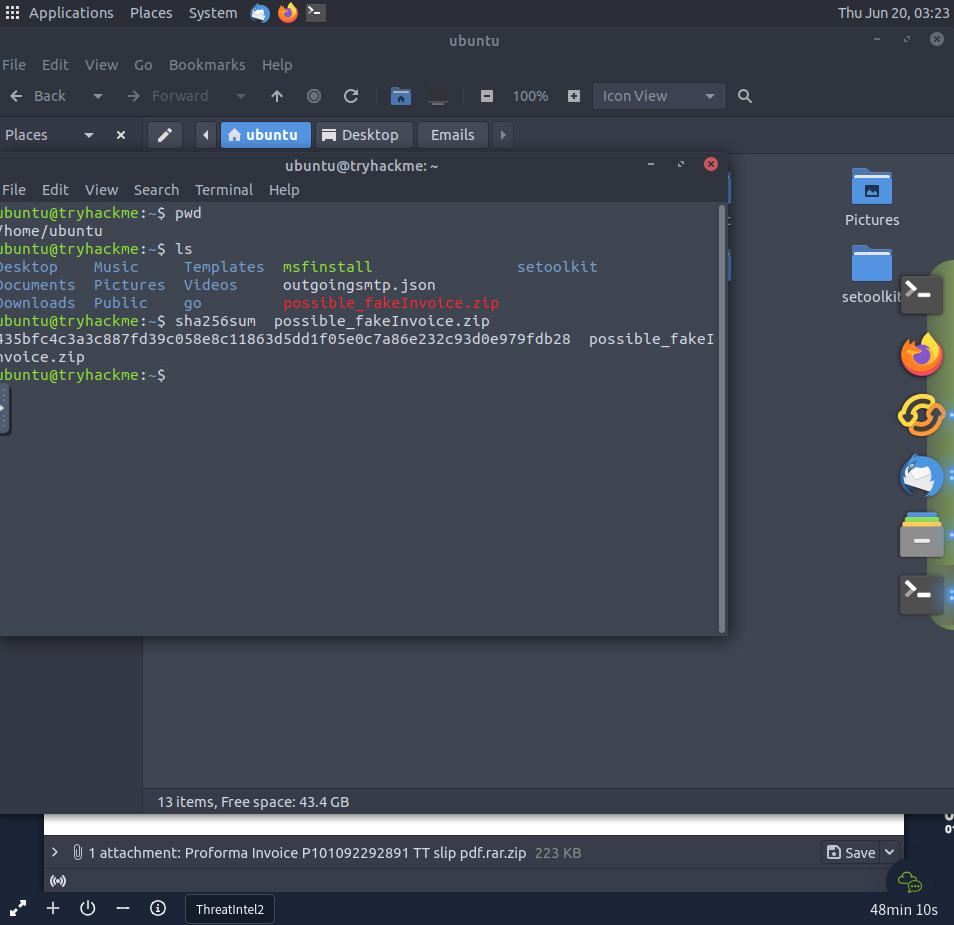
We’ll use Cisco Talos to find out what intelligence is in their database about the file. We’ll extract the sha256 hash from the file after downloading it.

I have renamed it as ‘possible\_fakeInvoice.zip’

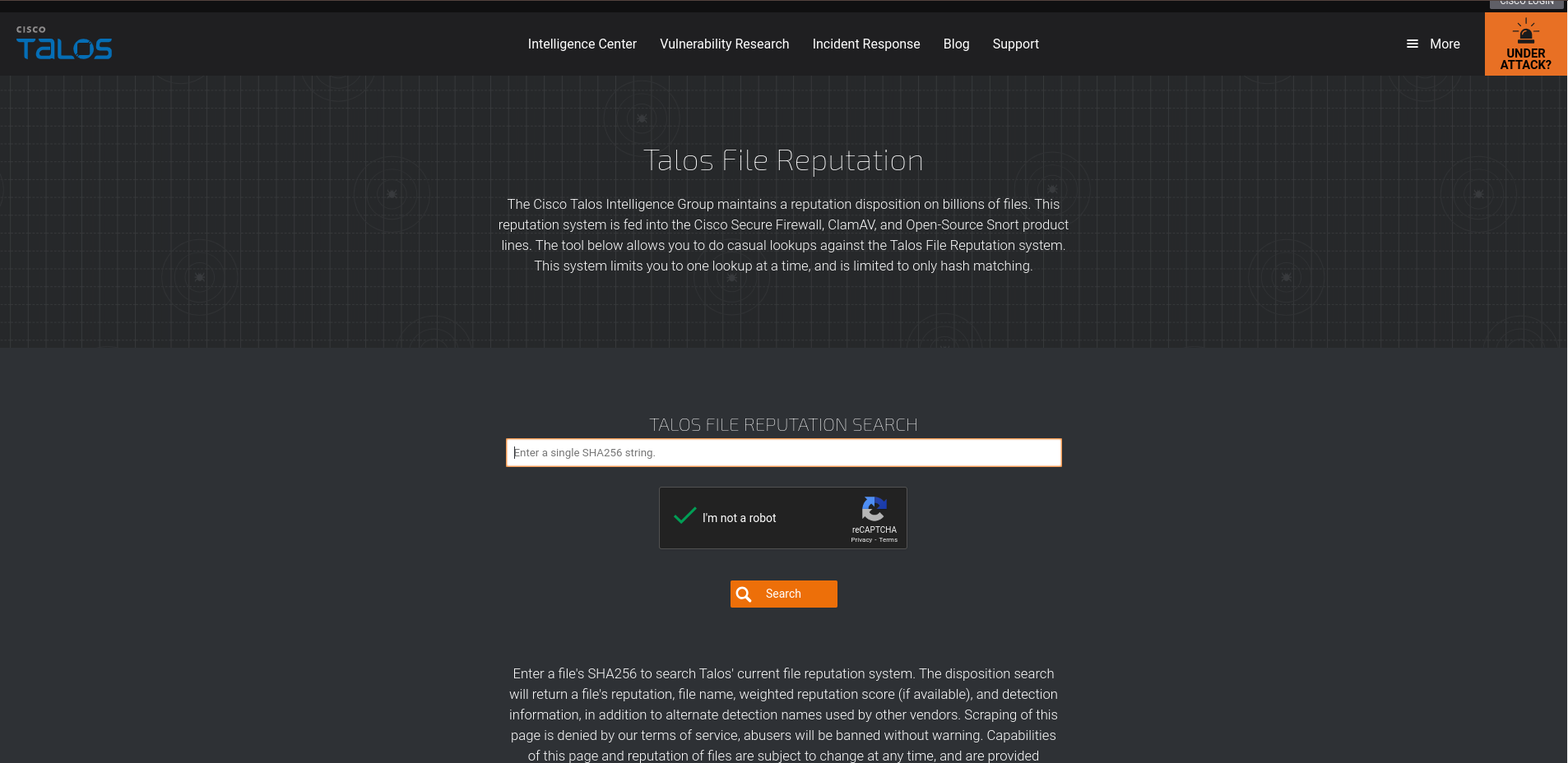


Now to extract the sha256 hash

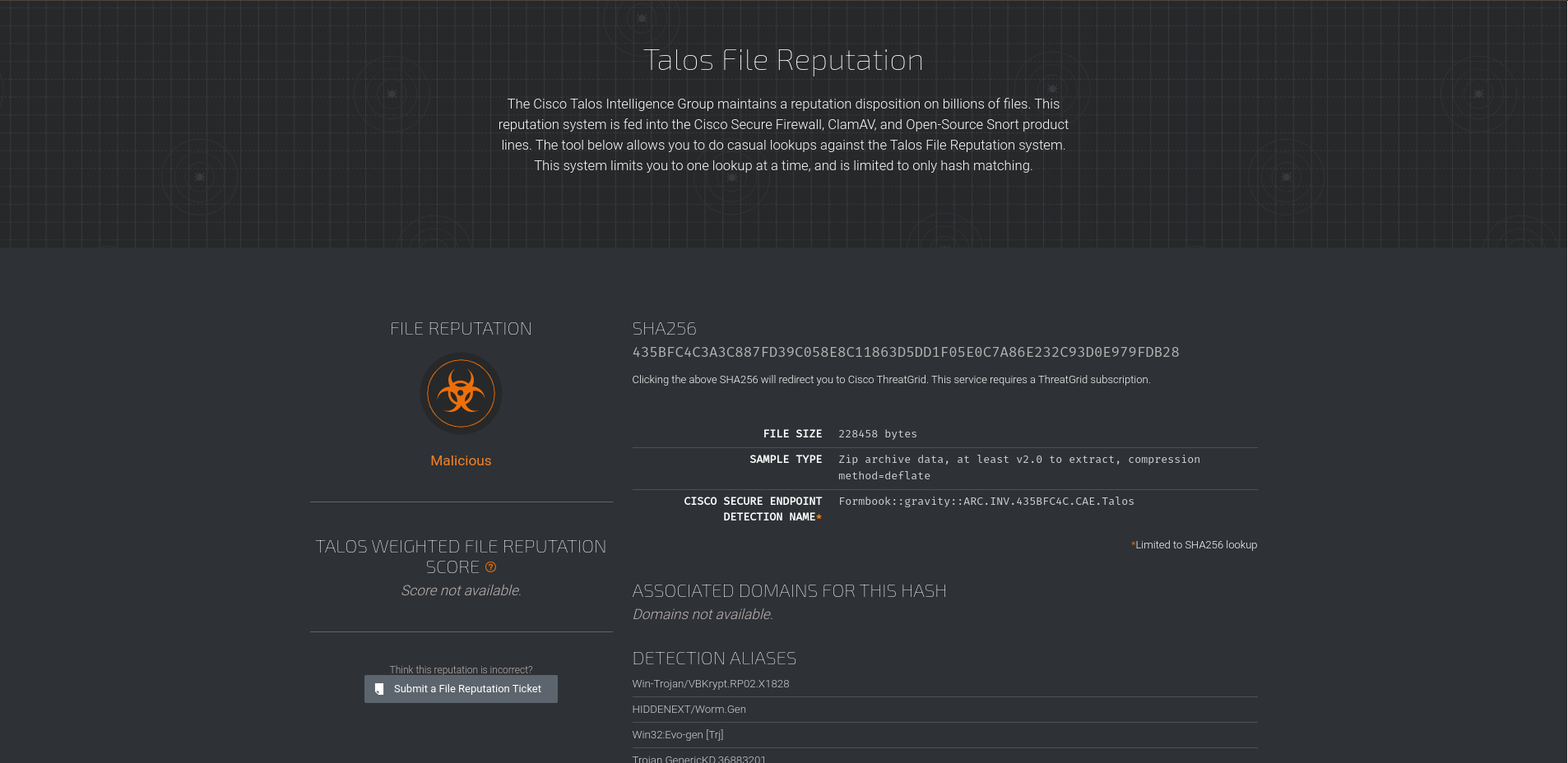




Now we lookup the hash in Cisco Talos ‘File Reputation’ database

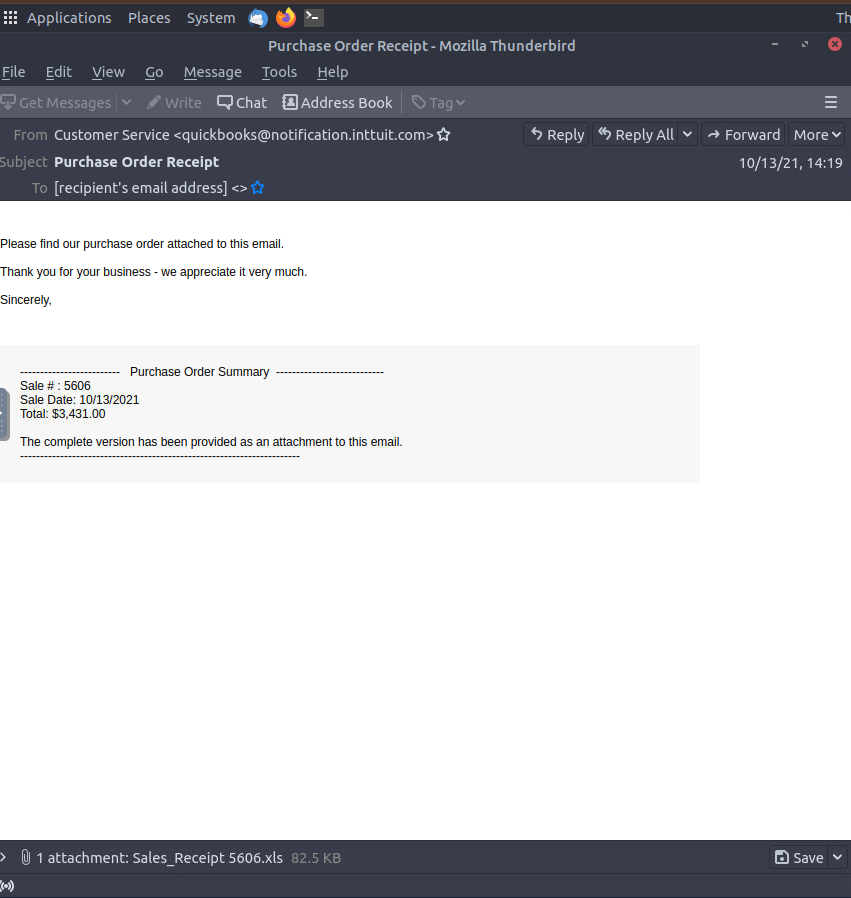


The file is confirmed to be malicious.



Appropriate mitigation measures must be taken.

Here is a malicious where the email closely resembles a company’s email address.

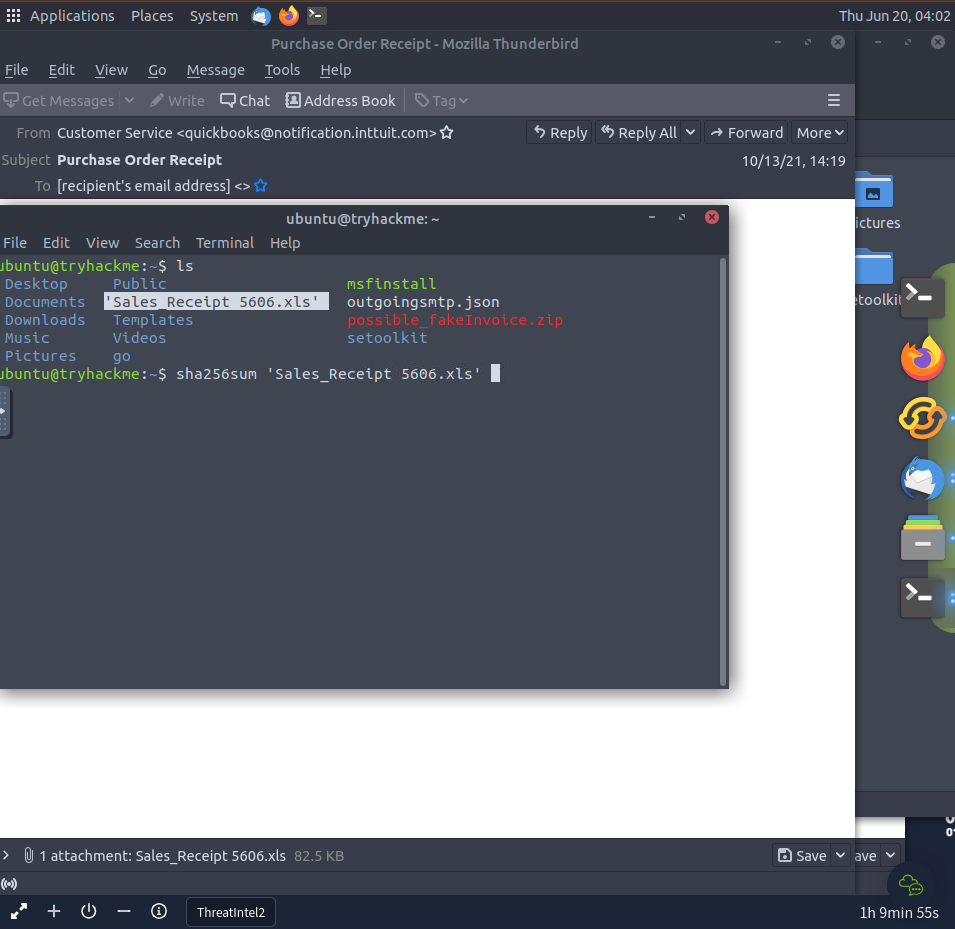


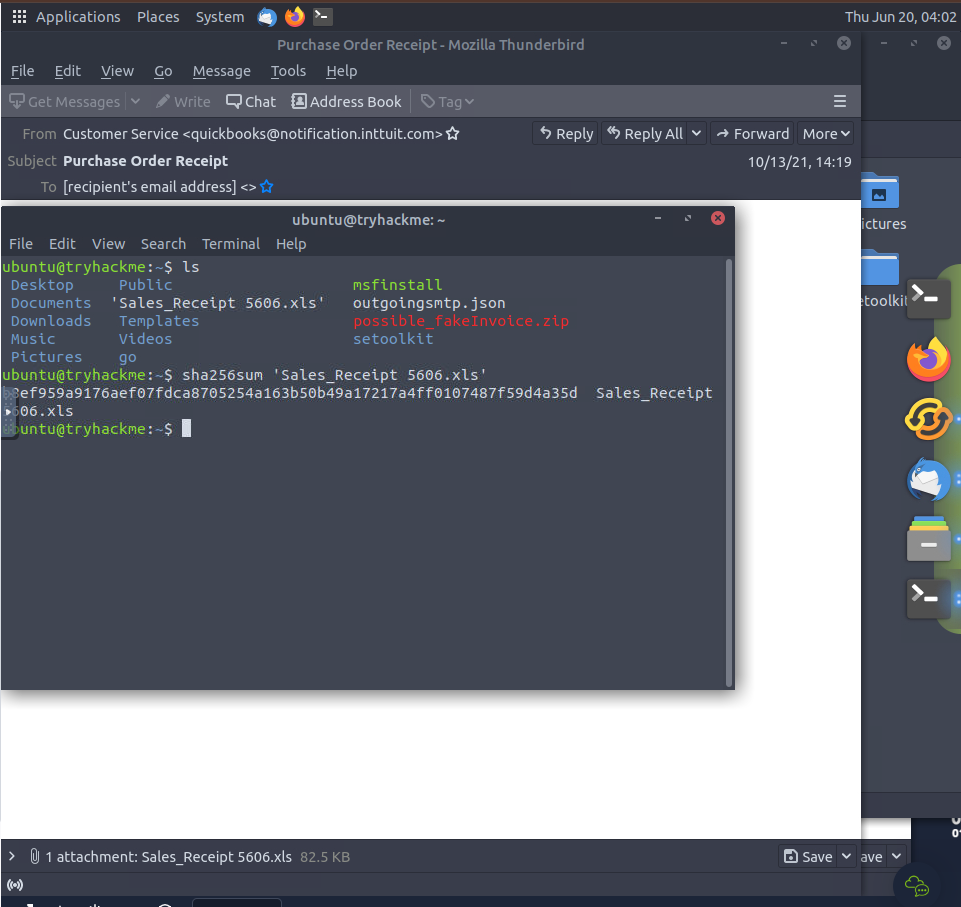
Let’s take in the details. We always start with the sender’s email address. The email looks official except for the extra ‘t’ at ‘…inttuit.com’.

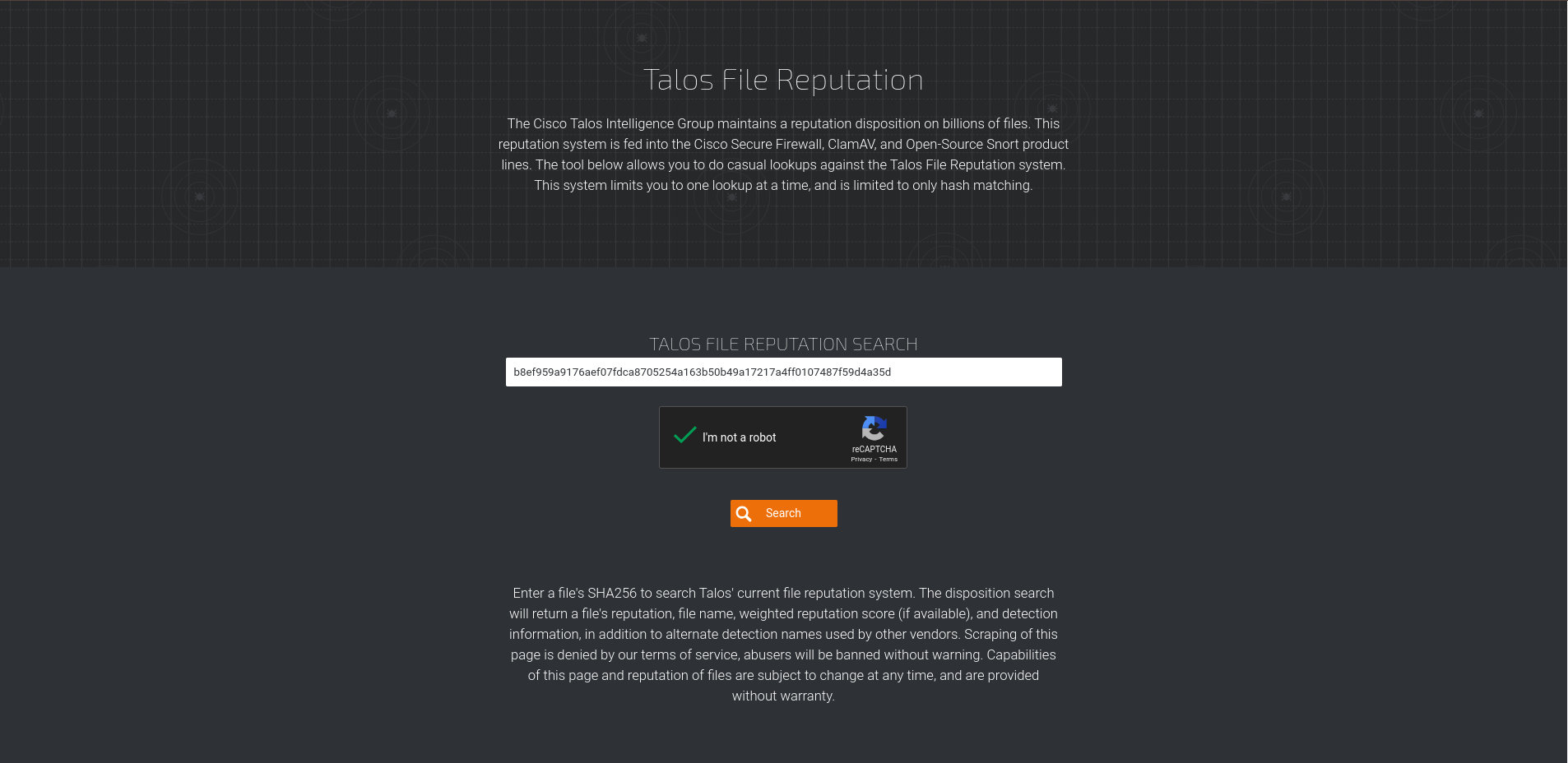


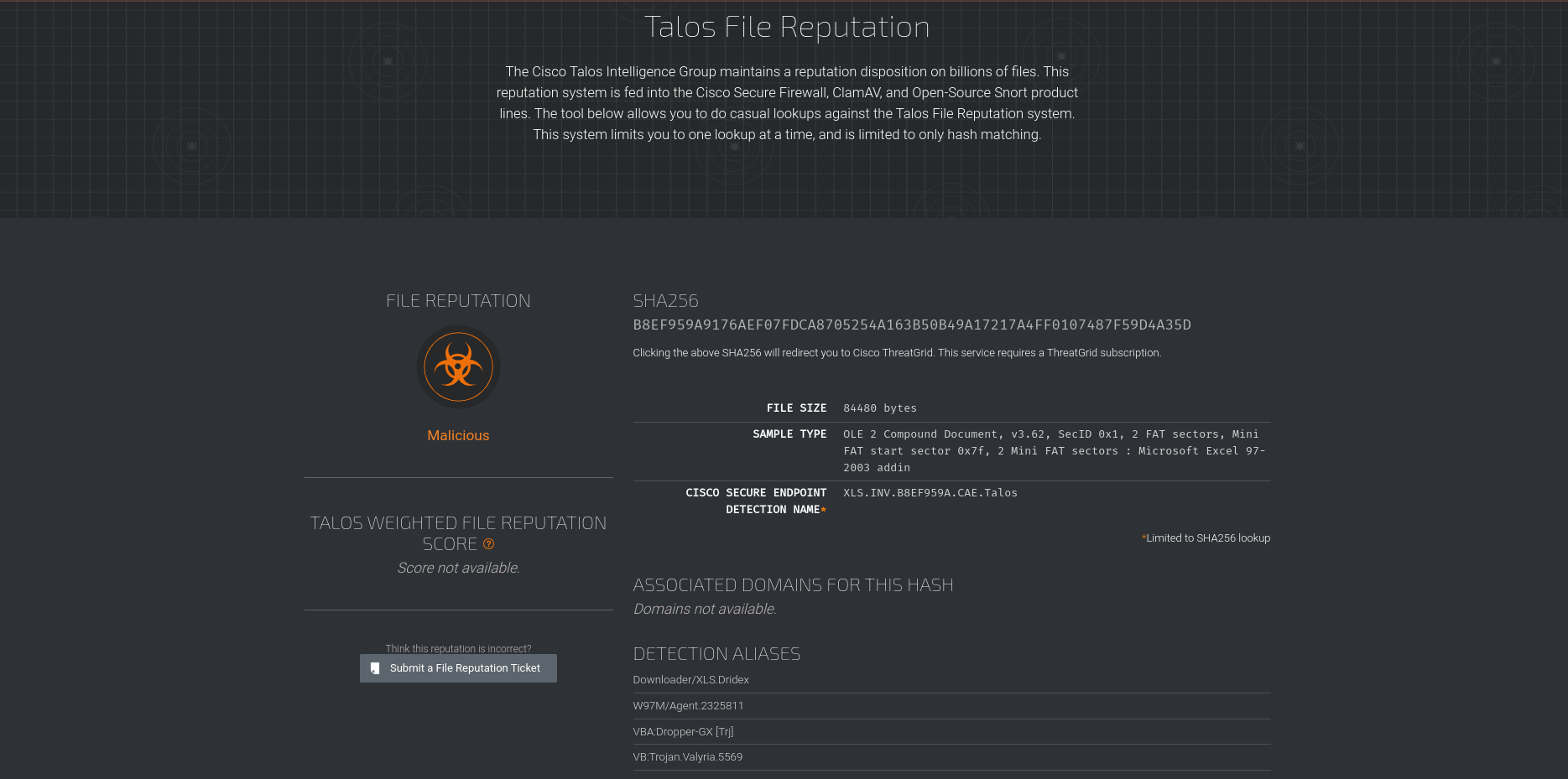
Mistakes of mistyping an email address are uncommon, and if they do happen, the entity sending the email will have to resend the email since they would not receive communication sent to the mistyped email.

We have reasonable suspicion. Let’s extract the sha256 hash and lookup the file’s reputation in Cisco Talos’ database.









The results from Cisco Talos confirm our suspicions. The file is malicious. The sender is a threat actor.

Appropriate mitigation measures must be taken.