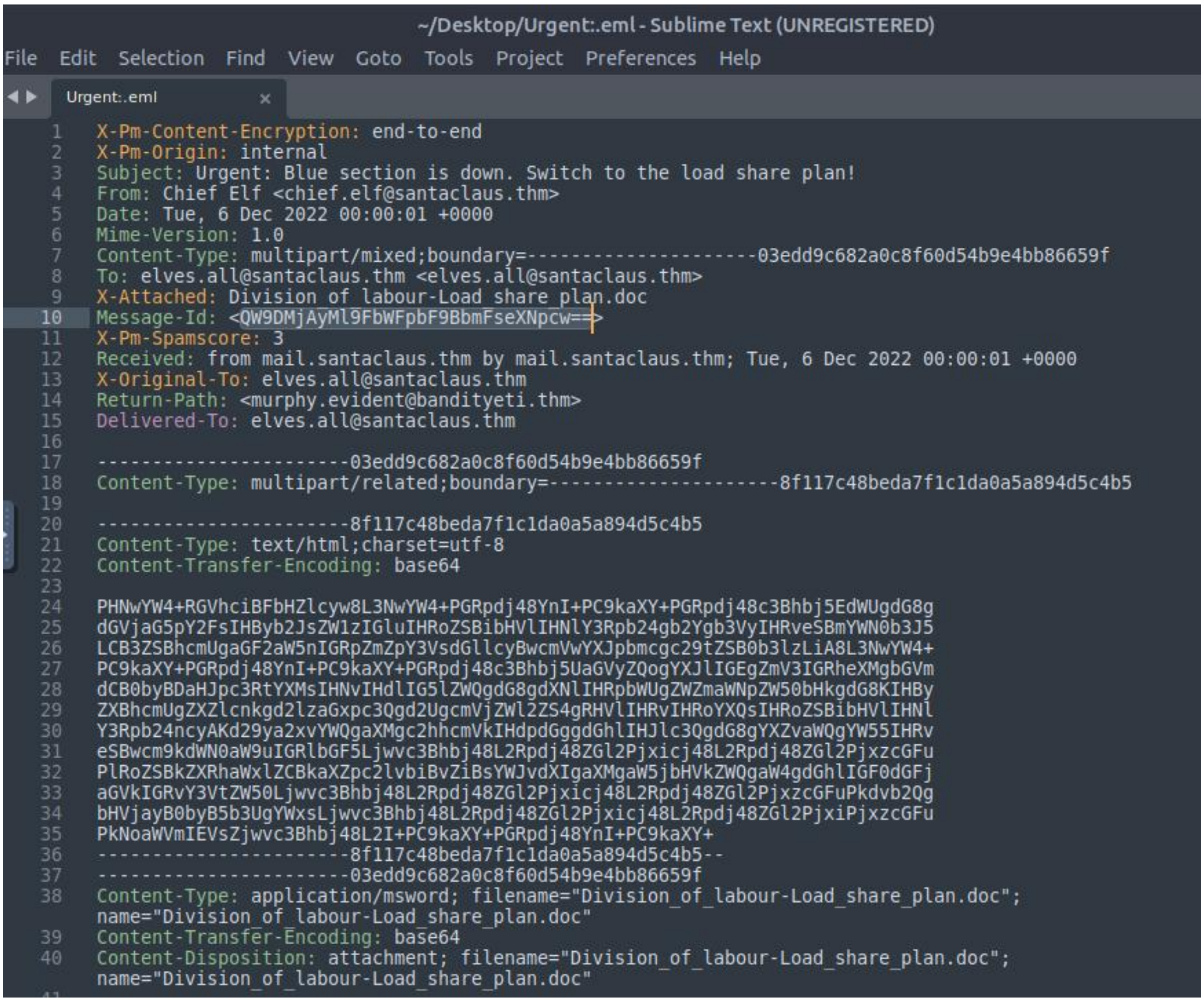
Advent of Cyber 2022

Day 6 – Email Analysis


~/Desktop/Urgent:.eml - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
Urgent:.eml

```
X-Pm-Content-Encryption: end-to-end
X-Pm-Origin: internal
Subject: Urgent: Blue section is down. Switch to the load share plan!
From: Chief Elf <chief.elf@santaclaus.thm>
Date: Tue, 6 Dec 2022 00:00:01 +0000
Mime-Version: 1.0
Content-Type: multipart/mixed;boundary=---------------------03edd9c682a0c8f60d54b9e4bb86659f
To: elves.all@santaclaus.thm <elves.all@santaclaus.thm>
X-Attached: Division of labour-Load share plan.doc
Message-Id: <QW9DMjAyMl9FbWFpbF9BbmFseXNpcw==>
X-Pm-Spamscore: 3
Received: from mail.santaclaus.thm by mail.santaclaus.thm; Tue, 6 Dec 2022 00:00:01 +0000
X-Original-To: elves.all@santaclaus.thm
Return-Path: <murphy.evident@banditdyeti.thm>
Delivered-To: elves.all@santaclaus.thm

-----------------------03edd9c682a0c8f60d54b9e4bb86659f
Content-Type: multipart/related;boundary=---------------------8f117c48beda7f1c1da0a5a894d5c4b5

-----------------------8f117c48beda7f1c1da0a5a894d5c4b5
Content-Type: text/html;charset=utf-8
Content-Transfer-Encoding: base64

PHNwYW4+RGVhciBFbHZlcyw8L3NwYW4+PGRpdj48YnI+PC9kaXY+PGRpdj48c3Bhbj5EdWUgdG8g
dGVjaG5pY2FsIHByb2JsZW1zIGluIHRoZSBibHVlIHNlY3Rpb24gb2Ygb3VyIHRveSBmYWN0b3J5
LCB3ZSBhcmUgaGF2aW5nIGRpZmZpY3VsdGllcyBwcmVwYXJpbmcgc29tZSB0b3lzLiA8L3NwYW4+
PC9kaXY+PGRpdj48YnI+PC9kaXY+PGRpdj48c3Bhbj5UaGVyZQogYXJlIGEgZmV3IGRheXMgbGVm
dCB0byBDaHJpc3RtYXMsIHNvIHdlIG5lZWQgdG8gdXNlIHRpbWUgZWZmaWNpZW50bHkgdG8KIHBy
ZXBhcmUgZXZlcnkgd2lzaGxpc3Qgd2UgcmVjZWl2ZS4gRHVlIHRvIHRoYXQsIHRoZSBibHVlIHNl
Y3Rpb24ncyAKd29ya2xvYWQgaXMgc2hhcmVkIGdpdGggdGhlIHJlc3QgdG8gYXZvaWQgYW55IHRv
eSBwcm9kdWN0aW9uIGRlbGF5Ljwvc3Bhbj48L2Rpdj48ZGl2Pjxicj48L2Rpdj48ZGl2PjxzcGFu
PlRoZSBkZXRhaWxlZCBkaXZpc2lvbiBvZiBsYWJvdXIgaXMgaW5jbHVkZWQgaW4gdGhlIGF0dGFj
aGVkIGRvY3VtZW50Ljwvc3Bhbj48L2Rpdj48ZGl2PjxicjwvZGl2PjxzcGFuPkdvb2Qg
bHVjayB0byB5b3UgYWxsLjwvc3Bhbj48L2Rpdj48ZGl2PjxicjwvZGl2PjxicjwvZGl2PjxiPjxzcGFu
PkNoaWVmIEVsZjwvc3Bhbj48L2I+PC9kaXY+PGRpdj48YnI+PC9kaXY+
-----------------------8f117c48beda7f1c1da0a5a894d5c4b5--
-----------------------03edd9c682a0c8f60d54b9e4bb86659f
Content-Type: application/msword; filename="Division_of_labour-Load_share_plan.doc";
name="Division_of_labour-Load_share_plan.doc"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="Division_of_labour-Load_share_plan.doc";
name="Division_of_labour-Load_share_plan.doc"
```

What is the email address of the sender?

chief.elf@santaclaus.thm

What is the return address?

murphy.evident@bandityeti.thm

On whose behalf was the email sent?

Chief Elf

What is the X-spam score?

3

What is hidden in the value of the Message-ID field?

AoC2022_Email_Analysis

Visit the email reputation check website provided in the task.
What is the reputation result of the sender's email address?

RISKY

Check the attachments.
What is the filename of the attachment?

Division_of_labour-Load_share_plan.doc

What is the hash value of the attachment?

0827bb9a2e7c0628b82256759f0f888ca1abd6a2d903acdb8e44aca6a1a03467

Visit the Virus Total website and use the hash value to search.
Navigate to the behaviour section.
What is the second tactic marked in the Mitre ATT&CK section?

Defense Evasion

Visit the InQuest website and use the hash value to search.
What is the subcategory of the file?

macro_hunter