📧 Phishing Report 1 – A Hope to CoCanDa

📝 Email Subject:

A Hope to CoCanDa

🧠 Header Analysis:

From Address:	billjobs@microapple.com
Return Path:	billjobs@microapple.com
IP Address:	93.99.104.210
SPF:	Fail
DKIM:	none
DMARC:	none

✉️ Email Body Content:

Hi TheMajorOnEarth

The abducted CoCanDians are with me including the President's daughter. Dont worry. They are safe in a secret location.Send me 1 Billion CoCanDs 🤑 in cash 💸 with a spaceship 🚀 and my autonomous bots will safely bring back your citizens.

I heard that CoCanDians have the best brains in the Universe. Solve the puzzle I sent as an attachment for the next steps.

I'm approximately 12.8 light minutes away from the sun and my advice for the puzzle is

"Don't Trust Your Eyes"

Lol 😂

See you Major. Waiting for the Cassshhhh 💰

🔍 Analysis Summary:

Key Red Flags - Urgency + Emotion , Money Demand , use emojis for distraction , solve the puzzle

🚨 IOCs (Indicators of Compromise):

IP Address:	**93.99.104.210**
Domain/URL:	Not found
Email Address:	billjobs@microapple.com
File Hash	Md5 - e47e8ea93468009e7449f2646fbca8ef SHA-1 - 71da5888ccba68b617ed6149cf62b297871d151c

File Name	PuzzleToCoCanDa.pdf

Tools Used:

PhishTool , VirusTotal, MxToolBox

Final Thoughts:

I analyse that this email have the file that contain malware , this email body contain the sci-fi style story and psychological trap that trick user to open this malicious attachment .