Mail Detector 7 Day

這則郵件的可信度如何？

我覺得……

APIs

hunter

VirusTotal

OpenAI

相關研究

過去的人都做了哪些酷東西

成果

我們做出來了？！

簡介

這到底在幹嘛？

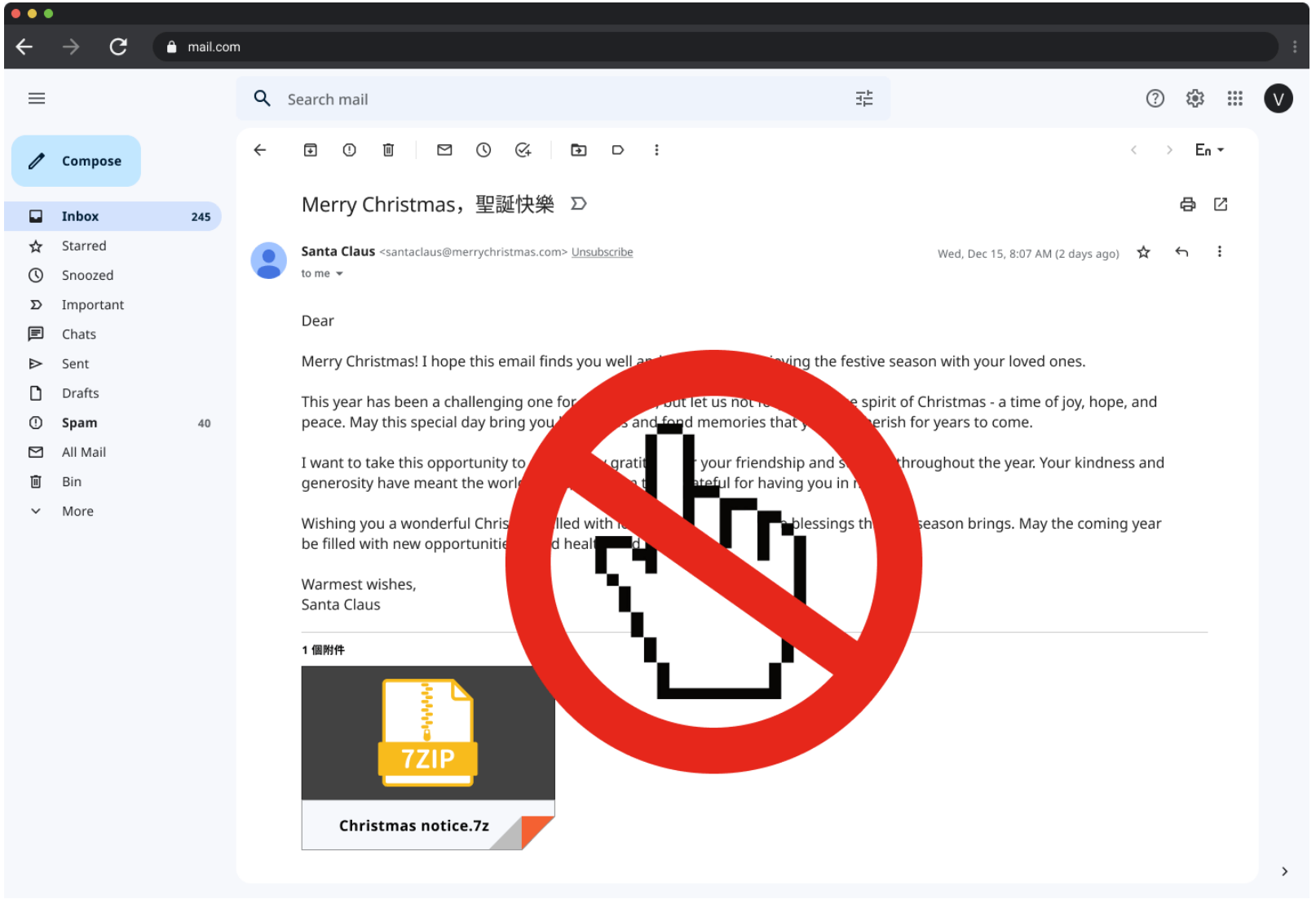
實作分享

我看不懂，
但我大受震驚

TeamT5偵查到中國駭客針對台灣金融單位的連續網路攻擊

- 以保單借款、聖誕節賀卡為主旨的魚叉式釣魚郵件展開攻擊行動、下載到 CobaltStrike Beacon(一種惡意軟體)進行攻擊

https://teamt5.org/tw/posts/press-release-chinese-adversaries-targeting-taiwan-financial-institutions/ [3]



TeamT5呼籲企業提高警覺心，留意釣魚信件

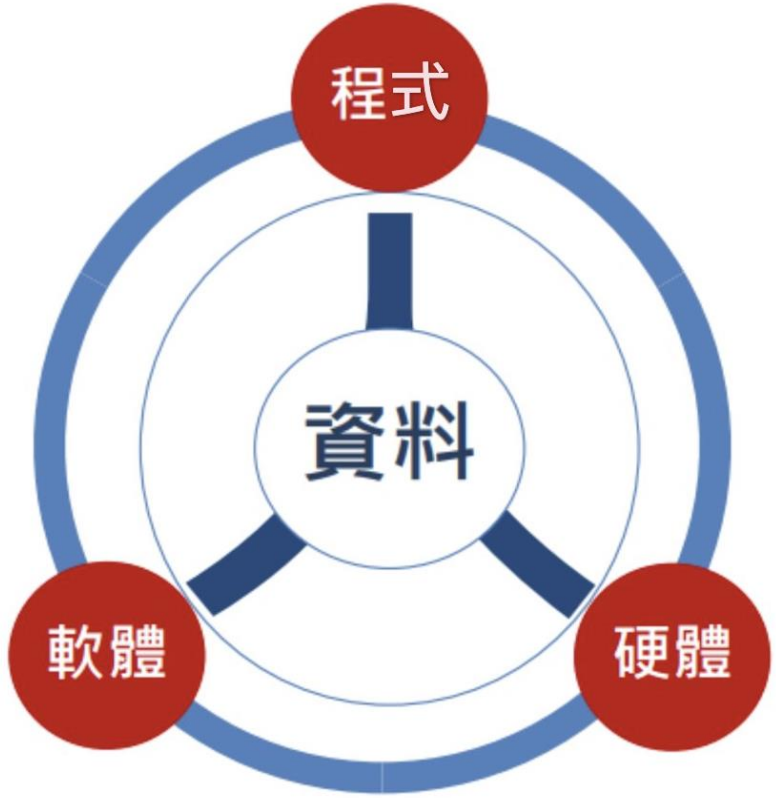
德國用戶遭遇釣魚攻擊 駭客假冒 CrowdStrike 修補通知

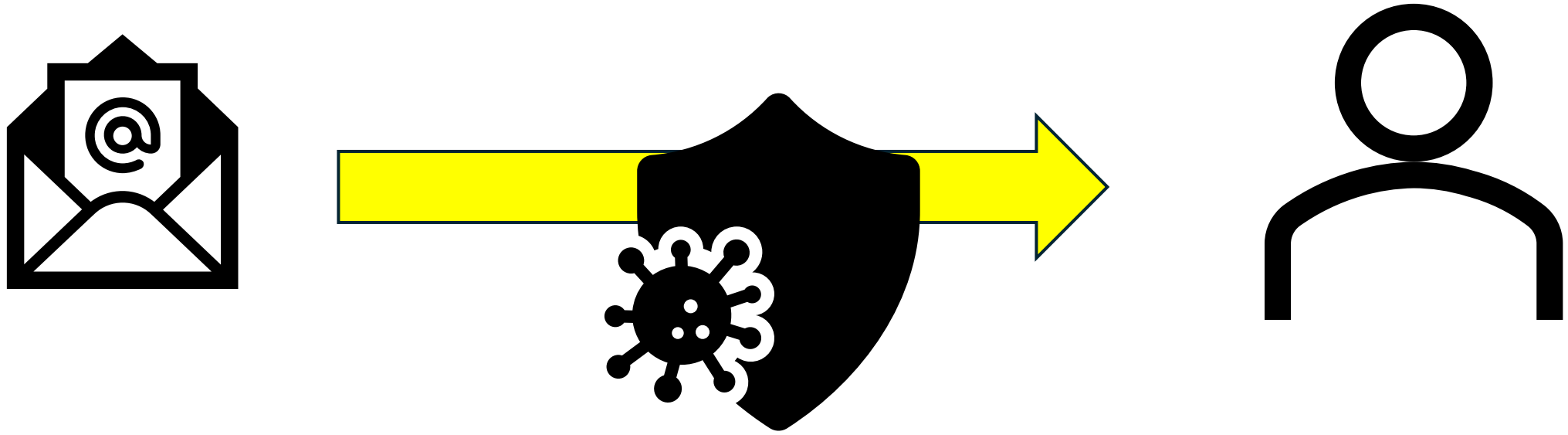
CrowdStrike更新引發全球電腦當機，駭客利用釣魚信件攻擊德國用戶。

https://netmag.tw/2024/07/30/german-users-face-phishing-attack [2]

誰最容易被攻擊？

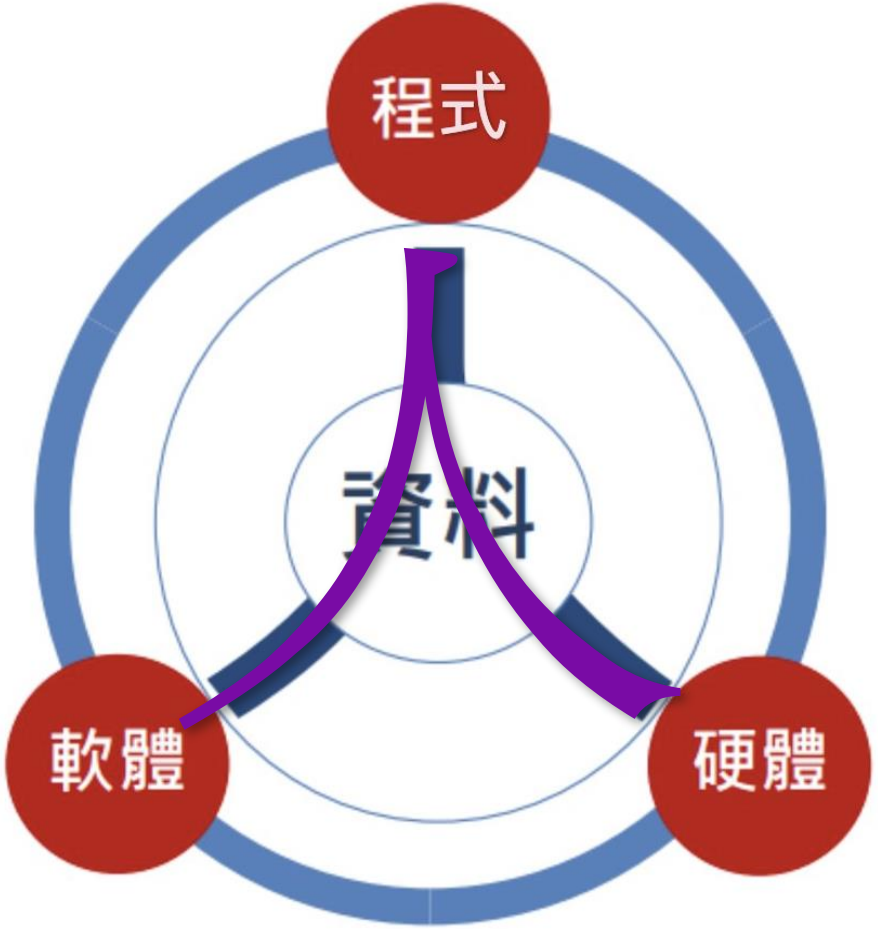
資料？硬體？程式？





誰最容易被攻擊？

人 是最重要的



目標客群

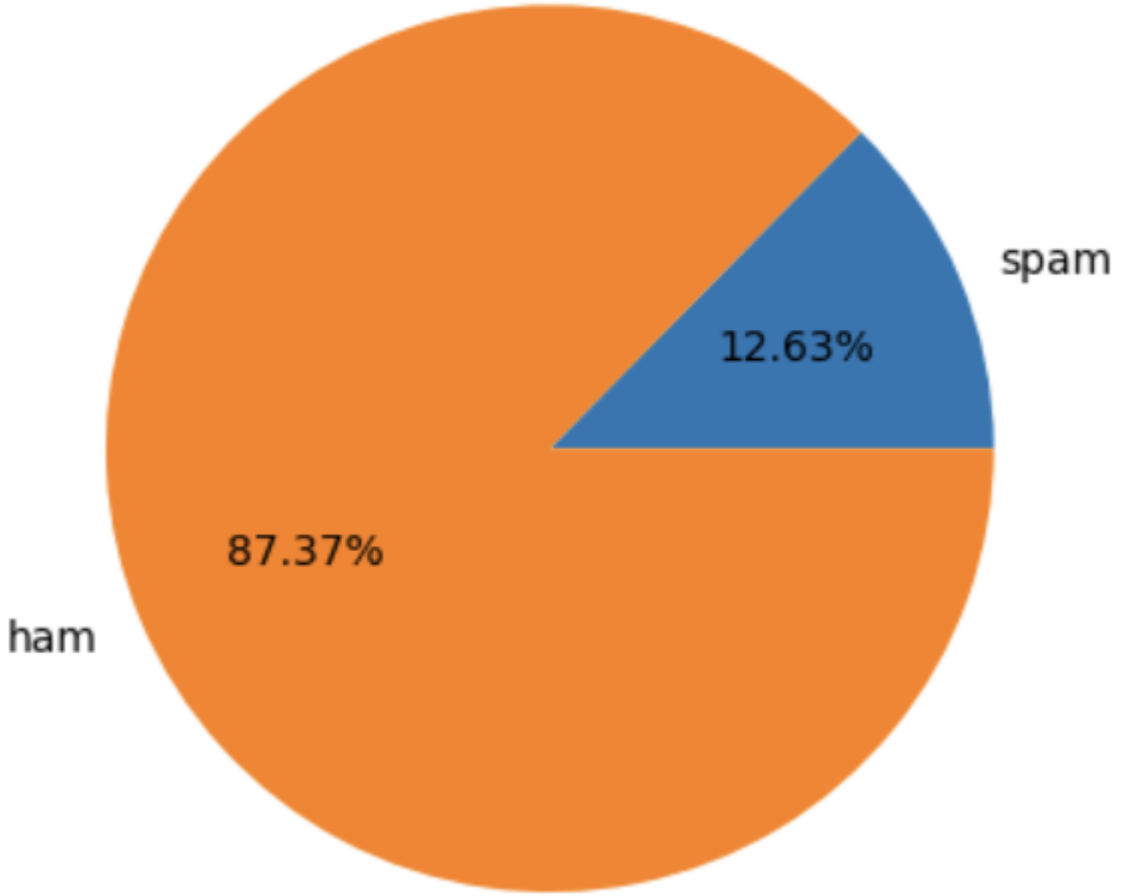
所有人！！！

相關研究

模型怎麼辦？

使用資料

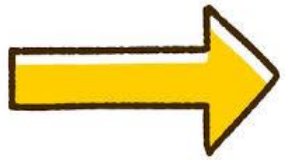
v1 class		v2 sms
ham spam	87% 13%	**5169** unique values
ham		Go until jurong point, crazy.. Available only in bugis n great world la e buffet... Cine there got a...
ham		Ok lar... Joking wif u oni...
spam		Free entry in 2 a wkly comp to win FA Cup final tkts 21st May 2005. Text FA to 87121 to receive entr...



SMS Spam Collection Dataset[7]

資料標記

v1 class		v2 sms
ham spam	87% 13%	**5169** unique values
ham		Go until jurong point, crazy.. Available only in bugis n great world la e buffet... Cine there got a...
ham		Ok lar... Joking wif u oni...
spam		Free entry in 2 a wkly comp to win FA Cup final tkts 21st May 2005. Text FA to 87121 to receive entr...



v1	v2
0	Go until jurong point, crazy.. Available only in bugis r
0	Ok lar... Joking wif u oni...
1	Free entry in 2 a wkly comp to win FA Cup final tkts 2
0	U dun say so early hor... U c already then say...
0	Nah I don't think he goes to usf, he lives around here
1	FreeMsg Hey there darling it's been 3 week's now an
0	Even my brother is not like to speak with me. They t
0	As per your request 'Melle Melle (Oru Minnaminungin
1	WINNER!! As a valued network customer you have be
1	Had your mobile 11 months or more? U R entitled to

網頁交互

OpenAI

LLM

RAG
Framework

LangChain + Chroma

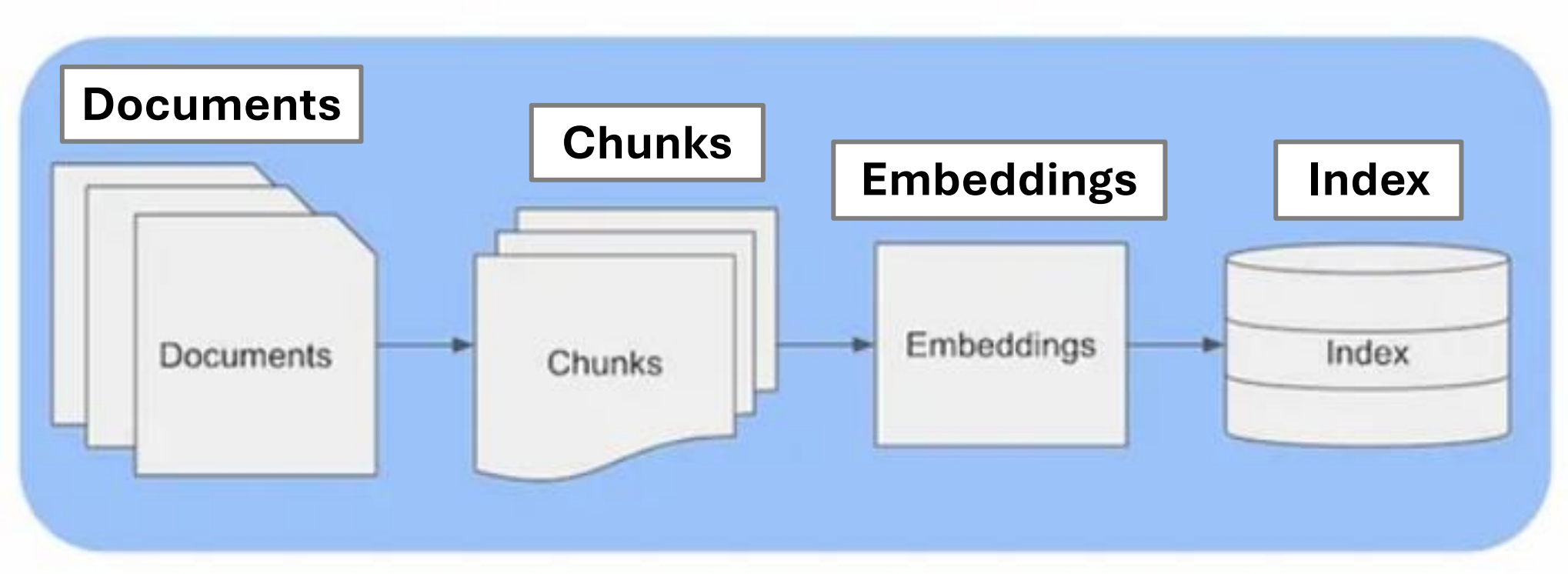
Chainlit

User
Interface

```
12      embedding = OpenAIEmbeddings()
13      if malicious_email_vectordb is None:
14          malicious_email_vectordb = Chroma(
15              persist_directory="components/malicious_email_vectordb", \
16              embedding_function=embedding)
17
18      runnable = prompt | model | StrOutputParser()
19
20      cl.user_session.set("malicious_email_vectordb", malicious_email_vectordb)
21      cl.user_session.set("runnable", runnable)
22      cl.user_session.set("embedding", embedding)
```

RAG

(Retrieval Augmented Generation)



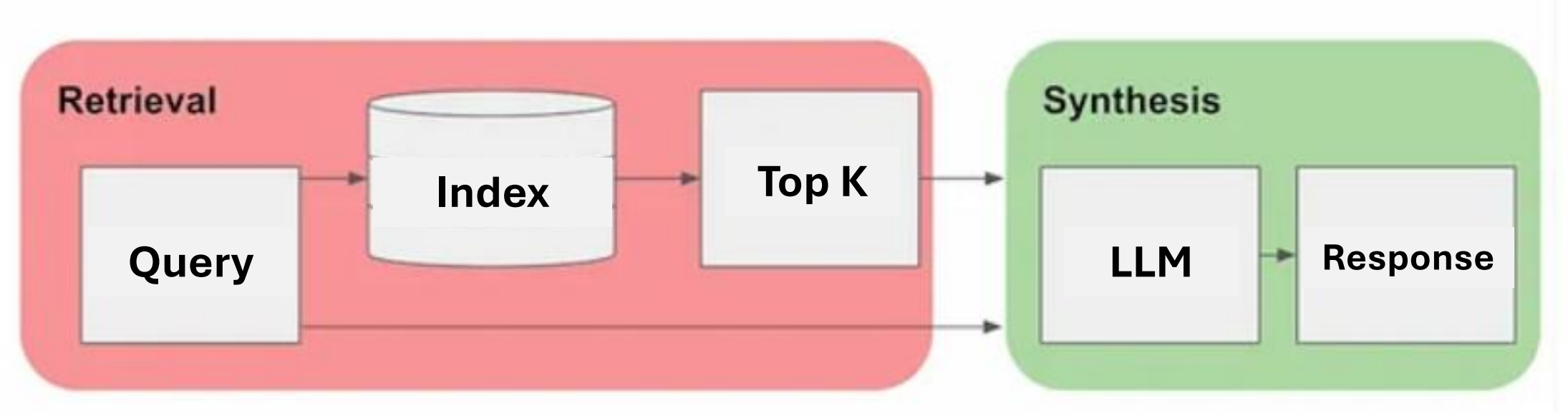
```python
embeddings = OpenAIEmbeddings(show_progress_bar=True)

file_path = 'components/train_spam.csv'
csv_data = pd.read_csv(file_path)
texts = csv_data['v2'].tolist()
metadatas = [{"malicious": label} for label in csv_data['v1'].tolist()]

CHUNK_SIZE = 100
vectordb = Chroma.from_texts(texts[:CHUNK_SIZE], embeddings,
                             metadatas=metadatas[:CHUNK_SIZE],
                             persist_directory="components/malicious_email_vectordb")

for i in range(CHUNK_SIZE, len(texts), CHUNK_SIZE):
    chunk_texts = texts[i:i+CHUNK_SIZE]
    chunk_metadatas = metadatas[i:i+CHUNK_SIZE]
    vectordb.add_texts(chunk_texts, metadatas=chunk_metadatas)
```

輸入比對



```
k=5
malicious_email_vectordb = cl.user_session.get("malicious_email_vectordb")
similar_docs = malicious_email_vectordb.similarity_search_with_score(content, k)

```

```python
async def analyze_attachments(attachments: List[Element]):
    tasks = [asyncio.create_task(VT_analyze_file(attachment.path)) f
    reports = await asyncio.gather(*tasks)
    detect_results = []
    for report, filename in zip(reports, [attachment.name for attach
        detect_results.append({
            "filename": filename,
            "antivirus_vendors_detect_type_count": {
                "malicious": report["data"]["attributes"]["stats"]["
                "suspicious": report["data"]["attributes"]["stats"][
                "undetected": report["data"]["attributes"]["stats"][
                "harmless": report["data"]["attributes"]["stats"]["h
            }
        })

    VT_attachments_analyze_prompt = f"Additionally, we have the resu
    reports: {detect_results}"
```

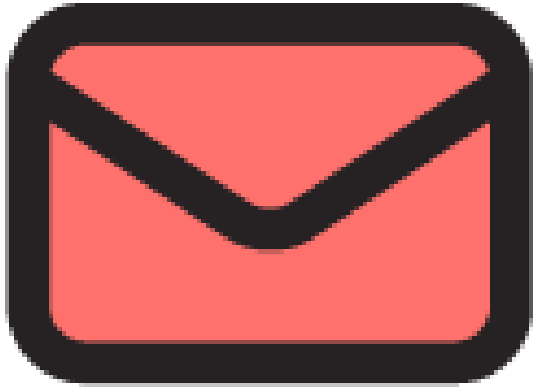
Few-Shot Prompting

```
175
176     examples = ""
177     for doc, score in similar_docs:
178         examples += f"Malicious: {doc.metadata['malicious']}\n"
179         examples += f"Content: {doc.page_content}\n\n"
180
181     email_content_prompt = f"Below are the email content, and the exa
182     email_content: {content}"
```

```python
runnable = cl.user_session.get("runnable")
msg = cl.Message(content="")
async for chunk in runnable.astream(
    {"examples": examples, "content": email_content_prompt + url_
):
    await msg.stream_token(chunk)

await msg.send()
```

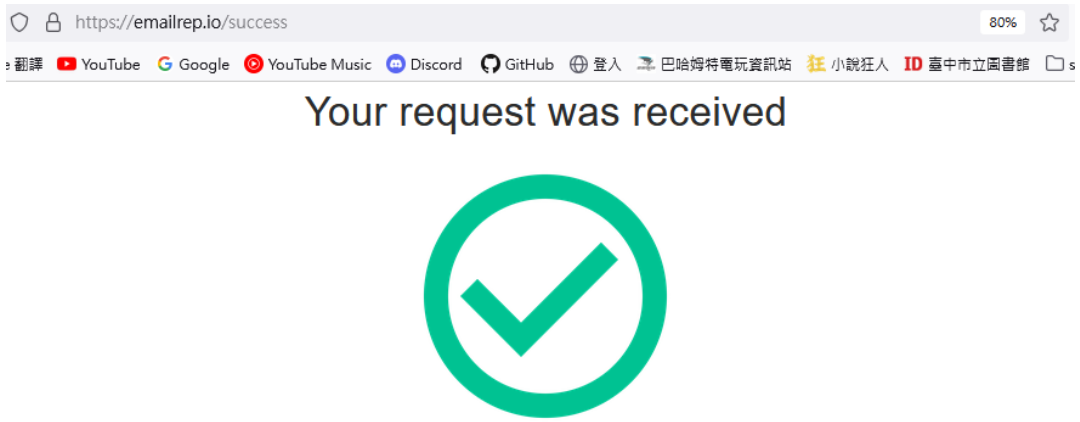
找一下資源



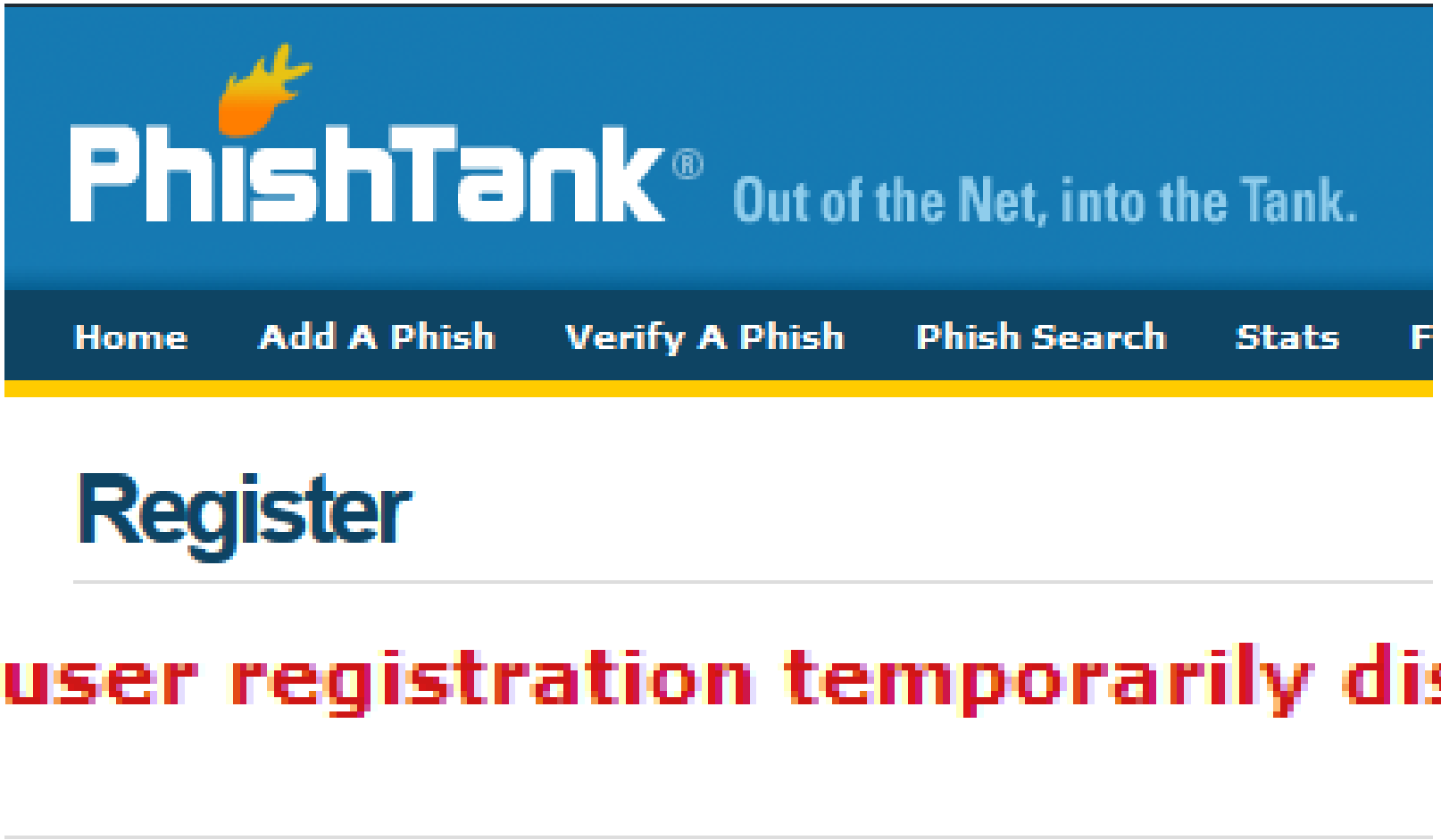
惡意郵件偵測項目

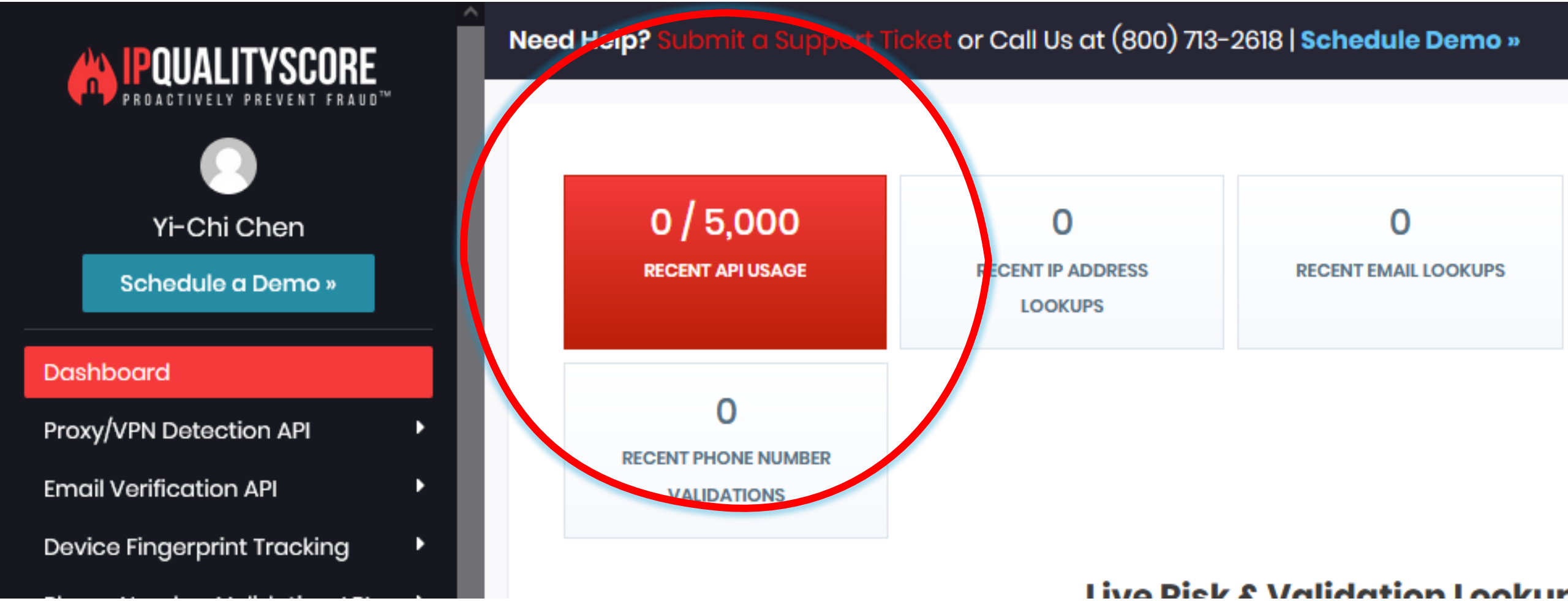
- 郵件內文描述
- 郵件中包含的連結
- 附件

需要審核


https://emailrep.io/success
80%
翻譯
YouTube
Google
YouTube Music
Discord
GitHub
登入
巴哈姆特電玩資訊站
小說狂人
臺中市立圖書館
Your request was received
If approved, we'll send your key to the email address you provided. Any questions or issues? Just let us know
Follow us on Twitter for news and updates.

不開放註冊


PhishTank®
Out of the Net, into the Tank.
Home
Add A Phish
Verify A Phish
Phish Search
Stats
Register
✗ New user registration temporarily disabled.


IPQUALITYSCORE
PROACTIVELY PREVENT FRAUD™
Yi-Chi Chen
Schedule a Demo »
Dashboard
Proxy/VPN Detection API
Email Verification API
Device Fingerprint Tracking
Need Help? Submit a Support Ticket or Call Us at (800) 713-2618 | Schedule Demo »
0 / 5,000
RECENT API USAGE
0
RECENT IP ADDRESS LOOKUPS
0
RECENT EMAIL LOOKUPS
0
RECENT PHONE NUMBER VALIDATIONS


hunter.io

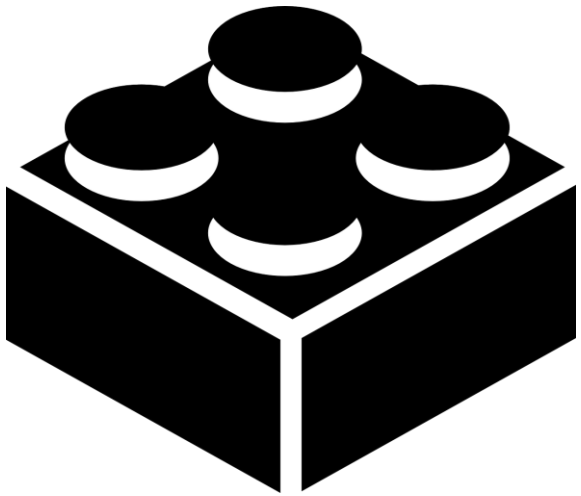
Hunter.io

- Email 評分
- 外部網站提及（公信力參考指標）

Virus total-API

- Domain 評分
- 郵件附檔分析

瀏覽器擴充功能



- 檢查郵件內文外部連結
- 寄件人信用評價
- 內文可信度分析

寄件人評分 by hunter.io

113年度AIS3 新型態資安實務暑期課程:最後行前通知! 收件匣 ×

Ais3 <service@ais3.org> Score: 100 Status: verify

7月26日 週五 下午1:29 (7 天

寄給

學員，您們好：
7/29下週一即將展開為期一週的AIS3 新型態資安實務暑期課程，以下為最後提醒注意事項

1.7/29請於9:00前報到 ，報到時請攜帶學生證，未滿18歲者請繳交家長同意書。
2.有申請7/28(日)提前一天住宿的同學，請於 7 / 28(日)17:00-18:00 於資訊館2樓國際會議廳

框選後彈出操作按鈕

這真的不是 P 上去的

學員，您們好：

7/29下週一即將展開為期一週的AIS3 新型

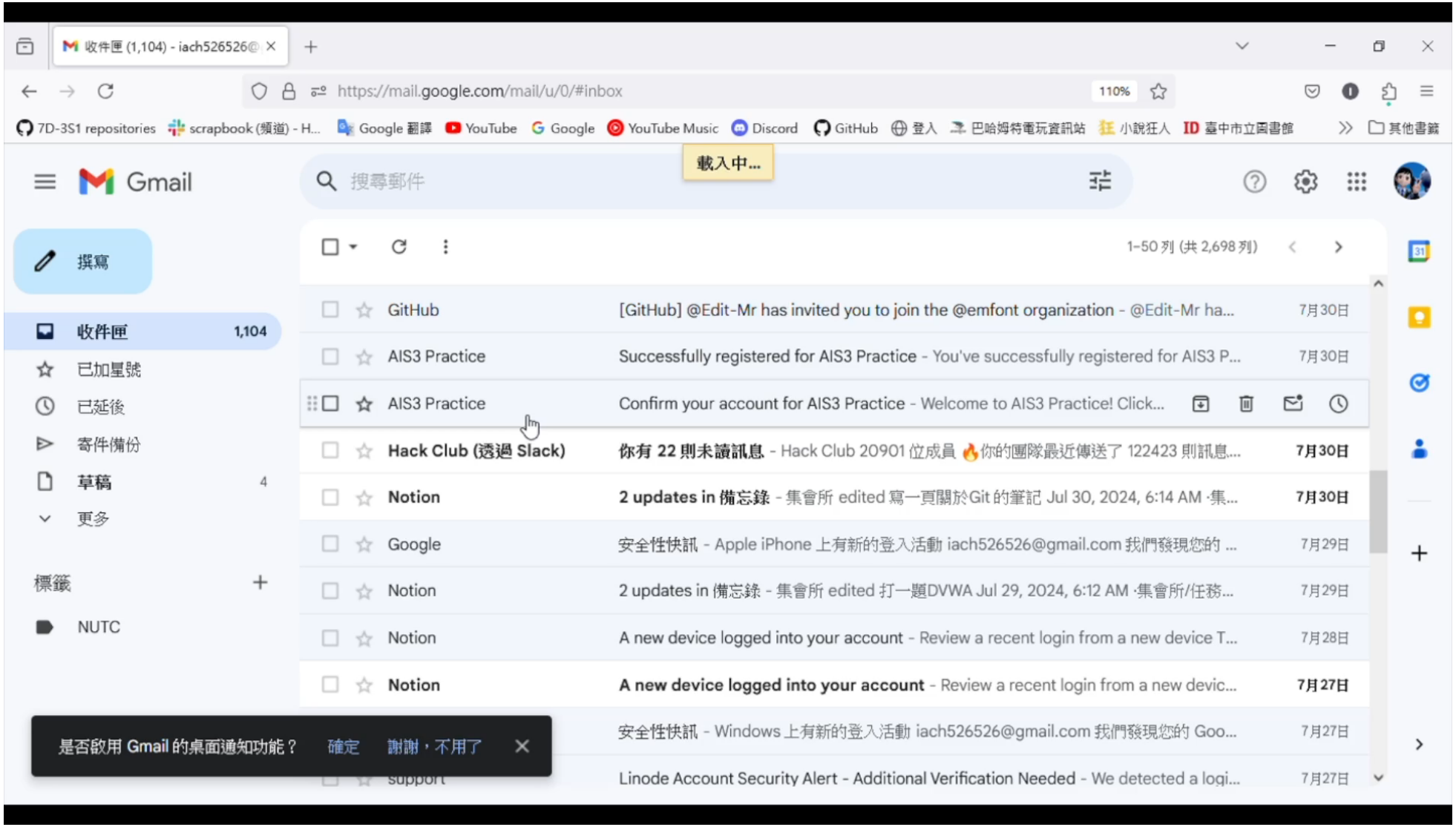
1.7/29請於9:00前報到，報到時請攜帶學

2.有申請7/28(日)提前一天住宿的同學，請

請提早告知。

3.申請住宿同學，請自[redacted]準備睡袋、盥洗用

成果展示


收件匣 (1,104) - iach526526@
https://mail.google.com/mail/u/0/#inbox
110%
7D-3S1 repositories
scrapbook (頻道) - H...
Google 翻譯
YouTube
Google
YouTube Music
Discord
GitHub
登入
巴哈姆特電玩資訊站
小說狂人
臺中市立圖書館
其他書籤
載入中...
Gmail
搜尋郵件
撰寫
收件匣 1,104
已加星號
已延後
寄件備份
草稿 4
更多
標籤
NUTC
1–50 列 (共 2,698 列)
GitHub [GitHub] @Edit-Mr has invited you to join the @emfont organization - @Edit-Mr ha... 7月30日
AIS3 Practice Successfully registered for AIS3 Practice - You've successfully registered for AIS3 P... 7月30日
AIS3 Practice Confirm your account for AIS3 Practice - Welcome to AIS3 Practice! Click...
Hack Club (透過 Slack) 你有 22 則未讀訊息 - Hack Club 20901 位成員 🔥你的團隊最近傳送了 122423 則訊息... 7月30日
Notion 2 updates in 備忘錄 - 集會所 edited 寫一頁關於Git的筆記 Jul 30, 2024, 6:14 AM ·集... 7月30日
Google 安全性快訊 - Apple iPhone 上有新的登入活動 iach526526@gmail.com 我們發現您的 ... 7月29日
Notion 2 updates in 備忘錄 - 集會所 edited 打一題DVWA Jul 29, 2024, 6:12 AM ·集會所/任務... 7月29日
Notion A new device logged into your account - Review a recent login from a new device T... 7月28日
Notion A new device logged into your account - Review a recent login from a new devic... 7月27日
安全性快訊 - Windows 上有新的登入活動 iach526526@gmail.com 我們發現您的 Goo... 7月27日
Linode Account Security Alert - Additional Verification Needed - We detected a logi... 7月27日
是否啟用 Gmail 的桌面通知功能？ 確定 謝謝，不用了

請輸入寄件者的電子郵件地址：

noreply@zoolab.org

請輸入要分析的郵件內容：

Welcome to AIS3 Practice!

Click the following link to confirm and activate your account:
http://ais3-
practic[redacted]

If the link is not clickable, try copying and pasting it into your browser.

從給定的信息來看，這封電子郵件並無可疑之處。

首先，發件人的信箱 noreply@zoolab.org 在分析後被認定為有效，且可以接收郵件。其得分為89，這表示該電子郵件地址的有效性非常高。

其次，電子郵件內容看起來像是一個帳戶確認或激活的過程，並無任何可疑的短語或語句。該郵件中的 URL 'http://ais3-practice.[redacted]' 也通過了安全檢查，並無任何防病毒軟體將其標記為惡意的或可疑的。

然而，即使這封郵件看起來不可疑，也應始終保持警惕，並遵循以下的安全提示：

1. 不要隨意點擊不明來源的電子郵件中的鏈接，尤其是來自您不認識的發件人的電子郵件。
2. 確保您的電腦和手機都安裝了最新的防病毒和防惡意軟體。
3. 如果您對某個電子郵件有任何疑問，最好直接聯絡該公司或組織，而不是通過電子郵件中的

被 Google 抓包了


恭喜成為 Google 的 第48763 位造訪用戶
垃圾郵件 ×
@gmail.com>
寄給 我
這封郵件有安全疑慮
我們發現有人曾利用類似郵件竊取使用者的個人資訊。請勿點選郵件中的連結、下載附件，也
看起來沒有問題

可疑連結

顯示與實際目的不符合


編輯連結
要顯示的文字：
Google.com
連結至：
網址
電子郵件地址
此連結應連至哪個 URL？
https://iach526526.github.io/html_project/
測試這個連結
不確定要在方塊中填入什麼？首先，在網路上找到您要連結的網頁 (使用搜尋引擎可能會有幫助)。 然後，複製瀏覽器網址列中的網址，貼到上述的方塊中。
取消
確定

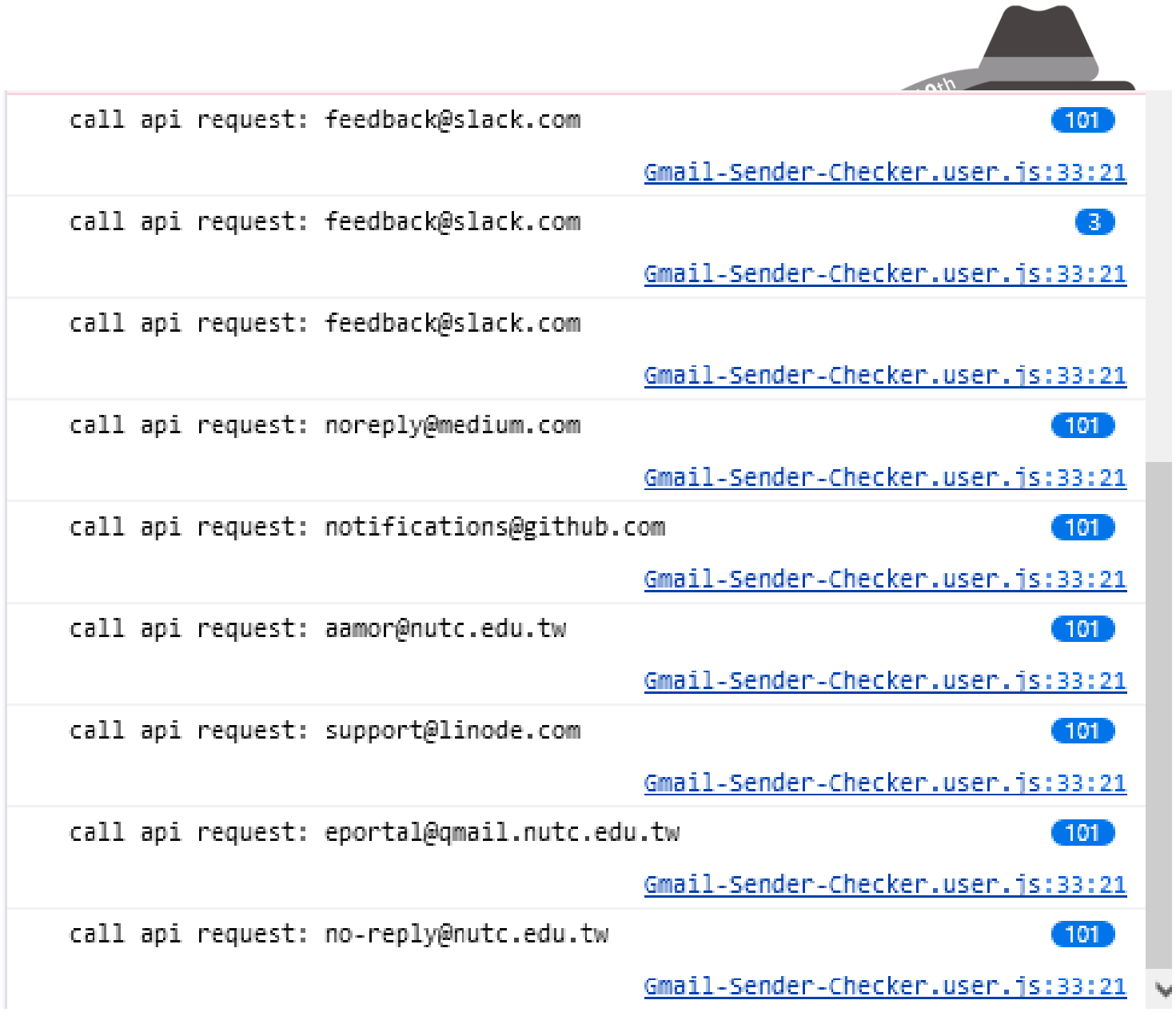
這封電郵看起來有一些可疑的地方。雖然該電郵來自一個Gmail帳戶，並有一個正確的DKIM簽名，但電郵內容中的連結"google.com"實際上指向的是"https://iach526526.github.io/html_project/"，這是一種常見的網路釣魚手法，詐騙者會利用這種方式引誘使用者點擊看似無害的連結，但實際上指向的是可能包含惡意軟件或用於收集個人信息的網頁。

從我們的病毒分析結果來看，該URL已經被68個病毒供應商掃描並認為是無害的，未被27個病毒供應商探測，沒有任何一個病毒供應商將其標記為惡意或可疑。這可能意味著該URL並未包含任何已知的惡意軟件，但這並不保證其絕對的安全性，因為新的或未被檢測到的惡意軟件可能不在病毒供應商的數據庫中。

一些挑戰 ~~鳥事~~

過多請求

請求 DOM 中的所有 mail



API 爆了

hunter

Hi each,

You have used all of your available verifications credits for the current period. Your verifications quota is scheduled to reset in about 1 month.

短網址無法直接處理，有沒有解碼的工具？


```
            },
            "date": 1722655277,
            "status": "completed",
            "stats": {
                "malicious": 0,
                "suspicious": 1,
                "undetected": 26,
                "harmless": 68,
                "timeout": 0
            }
        }
    },
    "meta": {
        "url_info": {
            "id": "26b2f9df1b97fe8c7ecaa4feab61e9f61ff5df79163b00921b9dc4c551b39726",
            "url": "https://reurl.cc/lyde76"
        }
    }
}
```


```
50 # Example usage
51 url_to_analyze = "bit-chasers.com"
52 report = analyze_url(url_to_analyze, API_KEY)
```


```
URL submitted successfully. Analysis ID: u-a3b55ef3
{
    "data": {
        "id": "u-a3b55ef35717b50be8e5d0afc34a3fe8bc
        "type": "analysis",
        "links": {
            "self": "https://www.virustotal.com/api
            "item": "https://www.virustotal.com/api
        },
        "attributes": {
            "stats": {
                "malicious": 12,
                "suspicious": 1,
                "undetected": 27,
                "harmless": 55,
                "timeout": 0
            },
```

開源庫，真酷

打個星星🌟吧🥺！

報告結束

附錄

參考資料

1.https://www.ithome.com.tw/news/160941
2.https://netmag.tw/2024/07/30/german-users-face-phishing-attack
3.https://reurl.cc/nv01l6
4.https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8907831
5.https://community.zextras.com/everything-you-need-to-know-about-dkim-for-your-carbonio-community-edition-servers/
6.LLM處理框架：https://medium.com/@daanish12069/pdf-chatbot-elevating-pdf-q-a-with-langchain-and-llama2-integration-7d592d99d365
7.垃圾郵件資料庫：SMS Spam Collection Dataset (kaggle.com)
8.資料處理流程：https://medium.com/@cch.chichieh/rag%E5%AF%A6%E4%BD%9C%E6%95%99%E5%AD%B8-langchain-llama2-%E5%89%B5%E9%80%A0%E4%BD%A0%E7%9A%84%E5%80%8B%E4%BA%BAllm-d6838febf8c4

相關研究

論文參考

A Comprehensive Survey for Intelligent Spam Email Detection

ASIF KARIM, SAMI AZAM, BHARANIDHARAN SHANMUGAM, KRISHNAN KANNOORPATTI, AND MAMOUN ALAZAB
College of Engineering, IT and Environment, Charles Darwin University, Casuarina, NT 0810, Australia
Corresponding author: Asif Karim (asif.karim@cdu.edu.au)

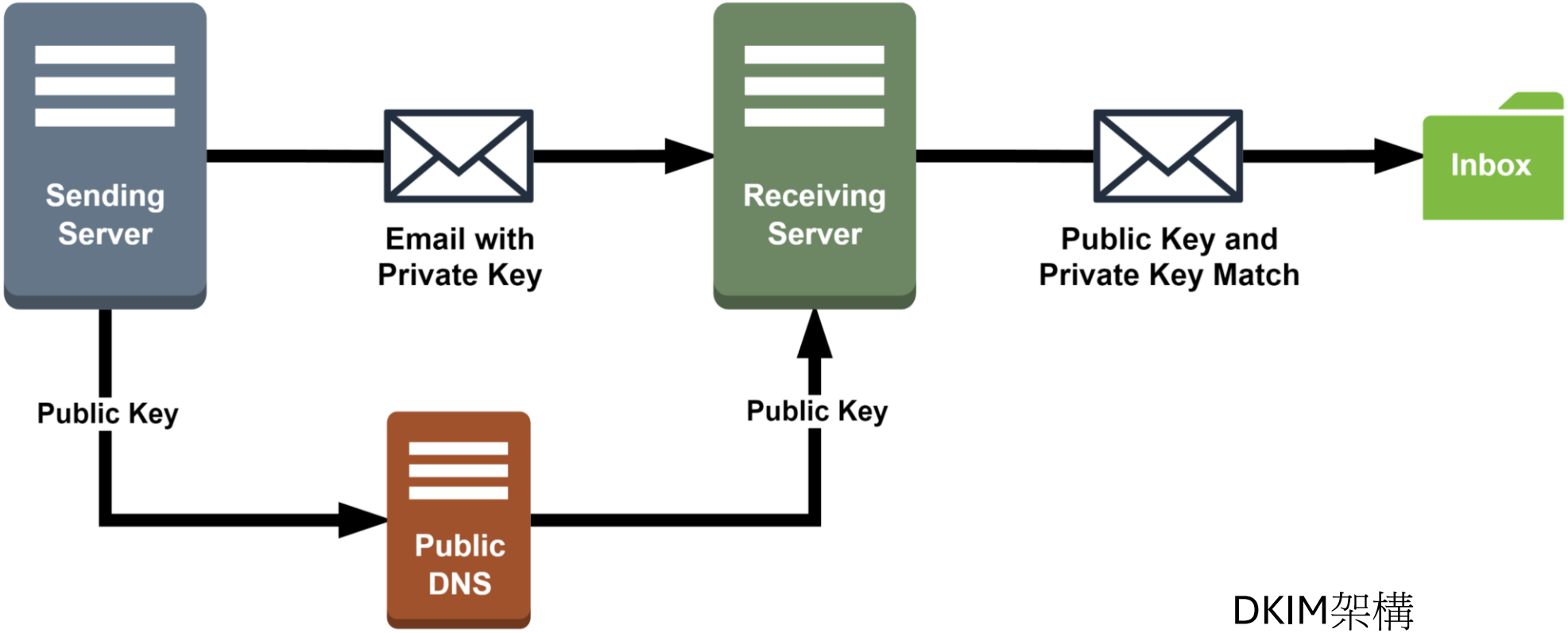
ieeexplore.ieee.org

https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8907831 [4]

相關研究

- DKIM
- SPF
- DMARC
- RBL

DKIM

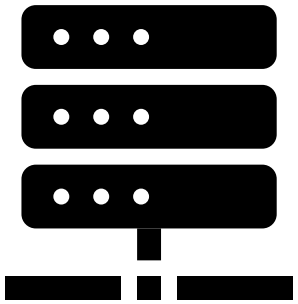


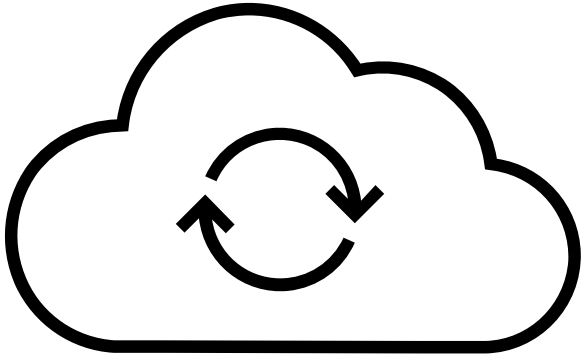
DKIM架構

https://reurl.cc/MjdN7p [5]

SPF

Hey, I want to bind my domain to 203.0.113.1





Foo.com

203.0.113.1/24

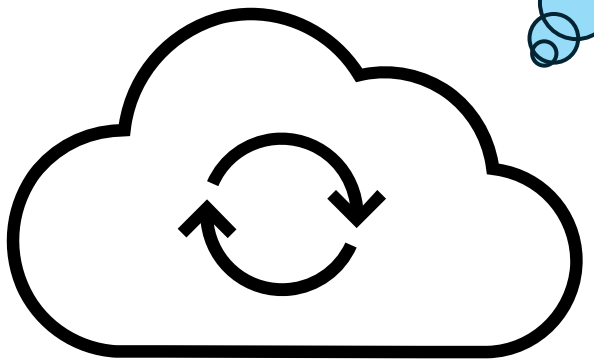
DNS server

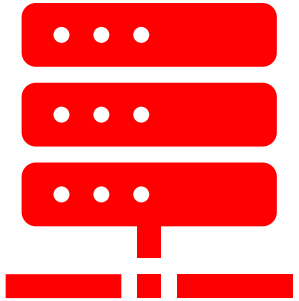
Domain	IP address
Foo.com	203.0.113.1/24
…	…

SPF

You are suspicous ...

Hey, I'm foo.com. I want send mail to iach@ais3.com





DNS server

Domain	IP address
Foo.com	203.0.113.1/24
...	...

foo.com

203.0.113.69/24

CSRF（Cross Site Request Forgery）

使用者在網站 A 上成功登入，並獲取一個認證 Cookie。

A
www...

Website

User 在未登出 A 網站的情況下瀏覽 B 網站

B

malicious Website

以 B Domain 以A 給User 的 Cookie 對 A 網站發送請求