

Threat Hunting

HW10

Name: 劉定睿 ID: M11409313

Date: 2025-11-24

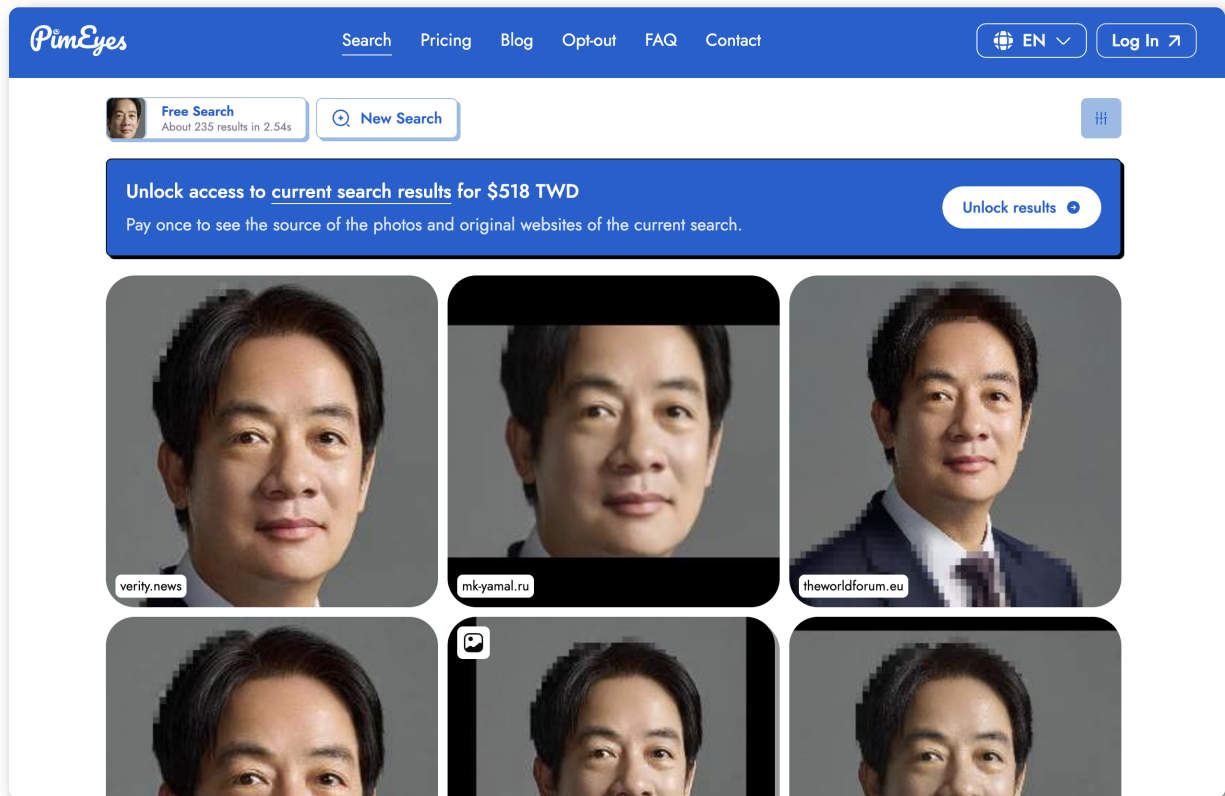
目錄

- [目錄](#)
- [Footprint Discovery](#)
 - [Protrait discovery](#)
 - [Email lookup](#)
- [Username Recon](#)
- [Data Leak Identification and Mitigation](#)

Footprint Discovery

Protrait discovery

I just searched for myself, but found no results matching my face. So, I tried searching for President Lai's picture.



- there's interesting that we can use AI tool can to seaching public person.

Gemini



who is this guy?

Analysis

您上傳的圖片人物是賴清德 (Lai Ching-te) 先生。

他是中華民國 (臺灣) 的現任總統 (President of the Republic of China (Taiwan))。

Email lookup

- I used Epieos to check my email and found that it had been exposed in a past data breach.

[redacted]@gmail.com [Download the data](#)

2 results (5.8 seconds) Wed, 19 Nov 2025 05:41:10 GMT

';--hibp? This tool allows you to find if an email address was leaked in data breaches.

Query	[redacted]@gmail.com
Found	1
Leaks	

[Subscribe](#)

EPIEOS

- use haveibeenpwned to search my email.

1 Data Breach

Oh no — pwned! This email address has been found in a data breach. Review the details below to see where your data was exposed.

Stay Protected
Notify Me

Get notified when your email appears in future data breaches

Internet Archive

In September 2024, the digital library of internet sites [Internet Archive](#) suffered a data breach that exposed 3.1M records. The breach exposed user records including email addresses, screen names and bcrypt password hashes.

Compromised data:

9月
2024年

- And there's some google account information of my email.

Google account finder will show you if the requested email is linked to a Google account and/or if the person left reviews on Google Maps.

Query

[redacted]@gmail.com

Photo

[https://lh3.googleusercontent.com/a-/\[redacted\]](https://lh3.googleusercontent.com/a-/[redacted])

Id

112-[redacted]

Last Update

2025-[redacted]

Services

Google Maps

[https://www.google.com/maps/contrib/\[redacted\]](https://www.google.com/maps/contrib/[redacted])

Google Calendar

[https://calendar.google.com/calendar/u/0/embed?src=\[redacted\]](https://calendar.google.com/calendar/u/0/embed?src=[redacted])

Google Plus Archive

[https://web.archive.org/web/*/plus.google.com/\[redacted\]](https://web.archive.org/web/*/plus.google.com/[redacted])

Username Recon

- jonafk555 is my nick name. I used peekyou to find the registration record.

The screenshot shows the 'peekyou' website interface. At the top, there are tabs for 'PEOPLE' and 'USERNAME', with 'USERNAME' selected. A search bar contains the text 'jonafk555' and a green 'Search' button. Below the search bar, the breadcrumb path is 'People Search > Username Search > jonafk555'. The main heading is 'Username Search Results for: jonafk555'. A red box highlights two buttons: '✓ 5 Profiles Found' and '27 Platforms Searched'. Other buttons include '100% Free Search' and 'Generate Usernames'. Under the heading, there is a section titled 'About Username jonafk555' with the following text: 'We checked username "jonafk555" across 50+ social media platforms and online services including Instagram, TikTok, Twitter, Facebook, LinkedIn, YouTube, and more. This username is taken on 5 platforms and available on 20 platforms. Note: Some platforms like Instagram and Facebook don't allow automated availability checks, so we show links to profiles we've found instead.'

- and again, AI is a best tool to find information.

The screenshot shows the Gemini AI chat interface. At the top, the name 'Gemini' is visible. A user input bubble contains the text 'jonafk555 是誰'. The AI response starts with a blue star icon and says: '您提到的是 jonafk555，根據我查到的資訊，這是一個在臺灣的 iT 邦幫忙 (iThome) 社群平台上的使用者帳號。' This is followed by two bullet points: '• 身份資訊：該帳號的個人資料顯示，這位使用者在現實生活中是一位學生，就讀於臺灣社會大學化學系。' and '• 平台等級：在 iT 邦幫忙上，該帳號被歸類為「iT 邦新手 4 級」。' The response continues: '鑑於您在「生物化學 (Biochemistry)」、「分析化學 (Analytical Chemistry)」等自然科學學門方面的專長，您可能是在尋找與這些領域相關的技術討論或文章。' and ends with the question: '請問您想了解 jonafk555 在 iT 邦幫忙上發布了哪些特定主題的內容或技術文章嗎？'

- bellincat is the biggest OSINT community in the world. they maintain a nice tool - WhatsMyName. It can find a lot of information of a nick name. The output is

unexpected.

WhatsMyName Web

OSINT COMBINE

Enter the username(s) in the search box, select any category filters & click the search icon or press CTRL+Enter

jonafk555

Category Filters

Active Filter: ALL

Found: 6 Processed: 741 / 741

Show Found Show False Positives Show Not Found Show All Open All Links

SITE	USERNAME	CATEGORY	LINK
BugCrowd	jonafk555	tech	https://bugcrowd.com/jonafk555
Docker Hub (Orga..)	jonafk555	coding	https://hub.docker.com/u/jonafk555
GitHub	jonafk555	coding	https://github.com/jonafk555
GitHub Gists	jonafk555	coding	https://gist.github.com/jonafk555
Gravatar	jonafk555	images	https://en.gravatar.com/jonafk555
TryHackMe	jonafk555	tech	https://tryhackme.com/r/p/jonafk555

Data Leak Identification and Mitigation

- First of all. Change password is the best method to prevent the attack by information leaked.

Google 帳戶

← 密碼

請選用高強度密碼；此外，切勿在其他帳戶中重複使用該密碼。瞭解詳情

系統可能會在某些裝置上將您登出帳戶。進一步瞭解哪些裝置會保留您的登入狀態

新密碼

密碼強度：
至少要有 8 個字元。請勿使用與其他網站帳戶相同的密碼，或是任何容易破解的密碼 (例如寵物的名字)。為什麼？

確認新密碼

變更密碼

- Later, we can check the "security activities" and find whether have abnormal login activity.

← 近期的安全性活動

過去 28 天內的安全性活動和快訊。 [瞭解詳情](#)

[發現不尋常的活動嗎？](#)

2025年11月14日

晚上9:08 在 Mac OS 裝置上有新的登入活動 台灣新北市
Mac OS [>](#)

2025年11月5日

上午10:59 在 Windows 裝置上有新的登入活動 Windows [>](#)

2025年10月25日

上午9:25 在 Windows 裝置上有新的登入活動 台灣新北市
Windows [>](#)

- And we can open "2 factor authentication".
If attacker obtain the leak password. 2FA can avoid the attacker to login to the system.

← 兩步驟驗證

您的帳戶受到兩步驟驗證功能的保護

開啟兩步驟驗證功能可為帳戶多設一道安全防護機制，防止駭客入侵。

除非您使用密碼金鑰登入，否則系統會要求您完成帳戶設定中安全性最高的第二個步驟。您隨時可以前往設定頁面更新第二個步驟和登入選項。 [前往安全性設定](#)



第二個步驟

請定期更新這些資訊並新增更多登入選項，確保您可以順利登入 Google 帳戶


密碼金鑰和安全金鑰 1 個安全金鑰 [>](#)

- We can also check the login device. And check whether have unclear device.


Google 帳戶

← 您的裝置

您目前已在下列裝置上登入帳戶，或過去 28 天內曾在這些裝置上登入帳戶。
同一部裝置可能會有多个活動工作階段。 [瞭解詳情](#)

 在 Mac 電腦上有 1 個工作階段
[什麼是工作階段?](#)

Mac OS
Google Chrome
新
✓ 目前的工作階段

 在 iPhone 上有 6 個工作階段
[什麼是工作階段?](#)

iPhone 台灣 1 小時前
iPhone 台灣 2 小時前
iPhone 台灣 2 小時前

- Third part application and service are also the risk of supply chain attack, we need to remove the unclear application to avoid attack.

Google 帳戶

← 第三方應用程式和服務

追蹤您帳戶與第三方之間的連結 

您目前與下列第三方應用程式和服務分享資料。 [瞭解詳情](#)

總共有 22 個應用程式/服務

篩選依據: ⓘ

使用 Google 帳戶登入 (21) 有權存取的项目 (5) 已連結帳戶 (0)

 Cake

- Turn Enhanced Safe Browsing on.

Google 帳戶

← 為您的帳戶啟用安全瀏覽強化防護功能

安全瀏覽強化防護功能

開啟「安全瀏覽強化防護功能」可更快速地主動防範危險的網站、下載內容和擴充功能，讓安全更有保障。[瞭解詳情](#)

您隨時可以關閉這項功能。

- And there's a nice function in Google. We can monitoring the darkweb intelligence.

Google



你正在監控暗網中的資料侵害事件

資料侵害結果摘要
未在暗網找到個資監控權中的資訊。

個人資料掃描結果
系統在暗網中發現個資監控權內的資訊。你新增了 3 種資訊 (共 5 種)。[編輯個資監控權](#)

名稱	0 筆結果	電話號碼	0 筆結果	電子郵件地址	0 筆結果
----	-------	------	-------	--------	-------