Threat Hunting

HW08

Name: 劉定睿 ID: M11409313

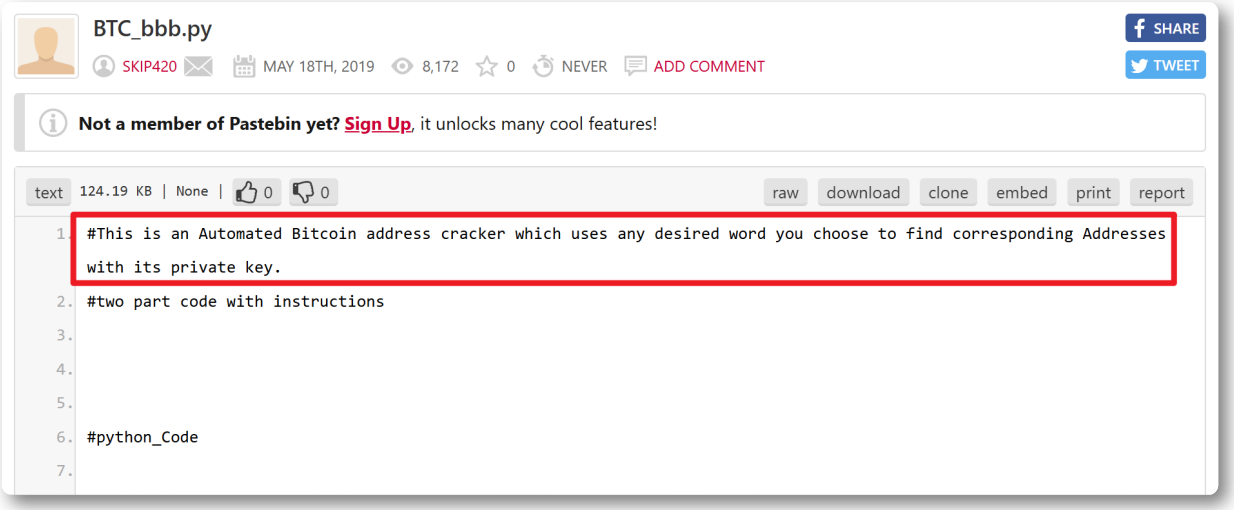
Date: 2025-11-10

目錄

Paste sites + Bitcointalk OSINT

Bitcoin address cracker

- Searching Statement: site:"pastebin[.]com" "公安"
- URL：https://pastebin.com/MXFShwzw
- Date：May 18th, 2019
- Why it's interesting?
    - Threat action groups can use it to crack bitcoin address in 2019.



- Indicators extracted:

```
description='A script to perform bruteforce dictionary attacks on brainwallets.'
```

- Confidence: Mid
- Safety/legality check: ilegal

wsjws[.]gzga[.]gov[.]cn - Police Officers Info Breached

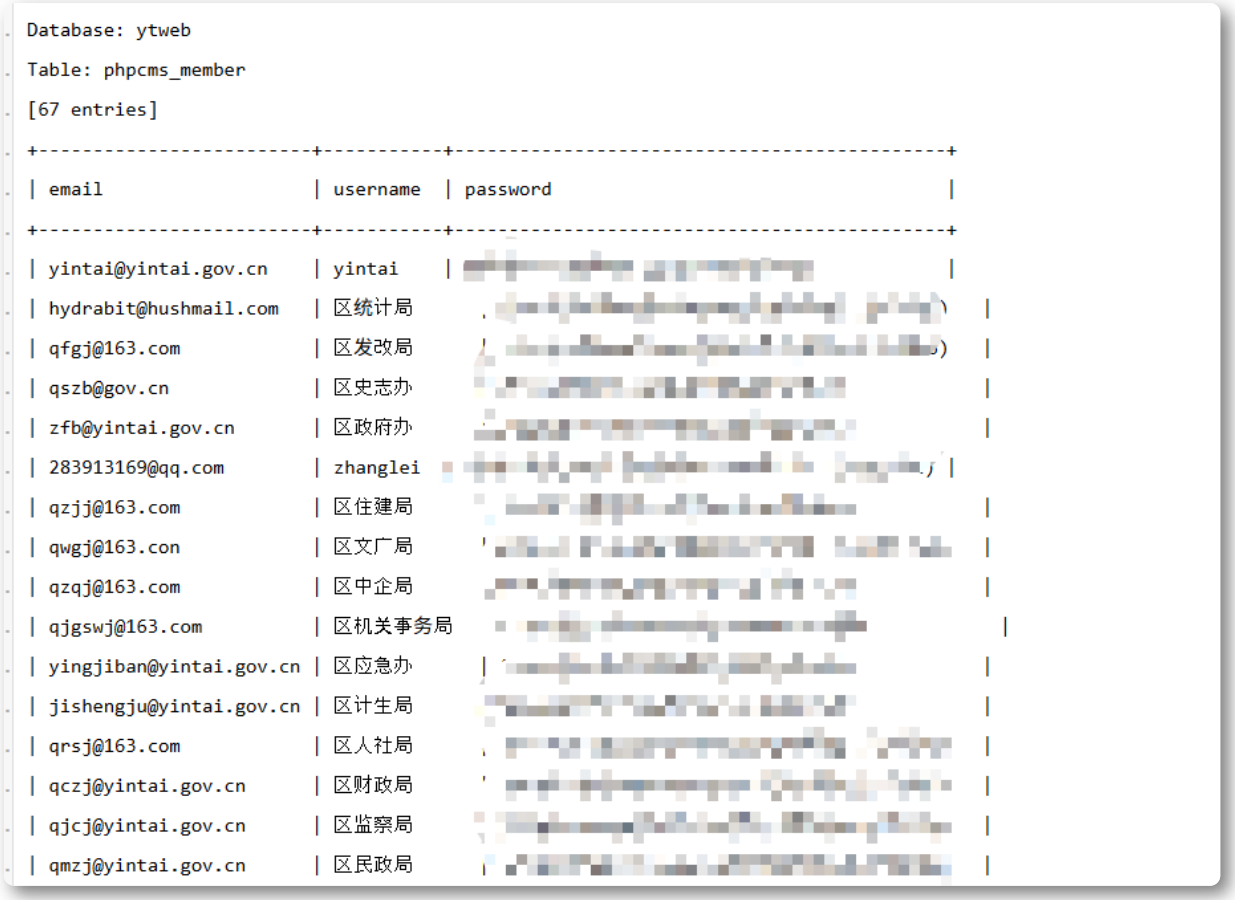
- Searching Statement: site:"pastebin[.]com" "公安"
- URL：https://pastebin.com/WCZiH95t
- Date：Oct 25th, 2014
- Why it's interesting?
    - fake data or political manipulate?

```
Database: NCMS_OnlinePolicingRoom
Table: OPR_BasicInfo
[266 entries]
+-----------------------------+-----------------------------------+-----------------------------------+------------
-------+-----------------------------------------+
| Fax                         | Email                             | WorkPhone                         | PolicName
| RingPhone                                |
+-----------------------------+-----------------------------------+-----------------------------------+------------
-------+-----------------------------------------+
| -                           | -                                 | 08543495016                       | 甲里派出所
| 08543495016                              |
| --                          | cs                                | 0854-6423812                      | 天台派出所
| 0854-6423812                             |
|  (0855) 5160110              | <blank>                            |  (0855) 5160110                    | 磻溪派出
所             | 110或0855—5160110                        |
```

- Indicators extracted:
  - clpcs2292110[@]163[.]com
  - panda7788520[@]163[.]com
  - hhgbjs[@]sina[.]com
  - ptxkps[@]163[.]com
- Confidence: Mid
- Safety/legality check: ilegal

yintai[.]gov[.]cn Hacked

- Searching Statement: site:"pastebin[.]com" "公安"
- URL：https://pastebin.com/0cyciR93
- Date：Oct 6th, 2014
- Why it’s interesting?
  - fake data or political manipulate?



```
Database: ytweb
Table: phpcms_member
[67 entries]
+-------------------------+-----------+-------------------------------------------+
| email                   | username  | password                                  |
+-------------------------+-----------+-------------------------------------------+
| yintai@yintai.gov.cn    | yintai    | [illegible]                               |
| hydrabit@hushmail.com   | 区统计局  | [illegible]                               |
| qfgj@163.com            | 区发改局  | [illegible]                               |
| qszb@gov.cn             | 区史志办  | [illegible]                               |
| zfb@yintai.gov.cn       | 区政府办  | [illegible]                               |
| 283913169@qq.com        | zhanglei  | [illegible]                               |
| qzjj@163.com            | 区住建局  | [illegible]                               |
| qwgj@163.con            | 区文广局  | [illegible]                               |
| qzqj@163.com            | 区中企局  | [illegible]                               |
| qjgswj@163.com          | 区机关事务局 | [illegible]                            |
| yingjiban@yintai.gov.cn | 区应急办  | [illegible]                               |
| jishengju@yintai.gov.cn | 区计生局  | [illegible]                               |
| qrsj@163.com            | 区人社局  | [illegible]                               |
| qczj@yintai.gov.cn      | 区财政局  | [illegible]                               |
| qjcj@yintai.gov.cn      | 区监察局  | [illegible]                               |
| qmzj@yintai.gov.cn      | 区民政局  | [illegible]                               |
```

- Indicators extracted:
  - jishengju[@]yintai[.]gov[.]cn
  - mfy[@]yintai[.]gov[.]cn
  - 228602600[@]QQ[.]com
- Confidence: Mid
- Safety/legality check: ilegal

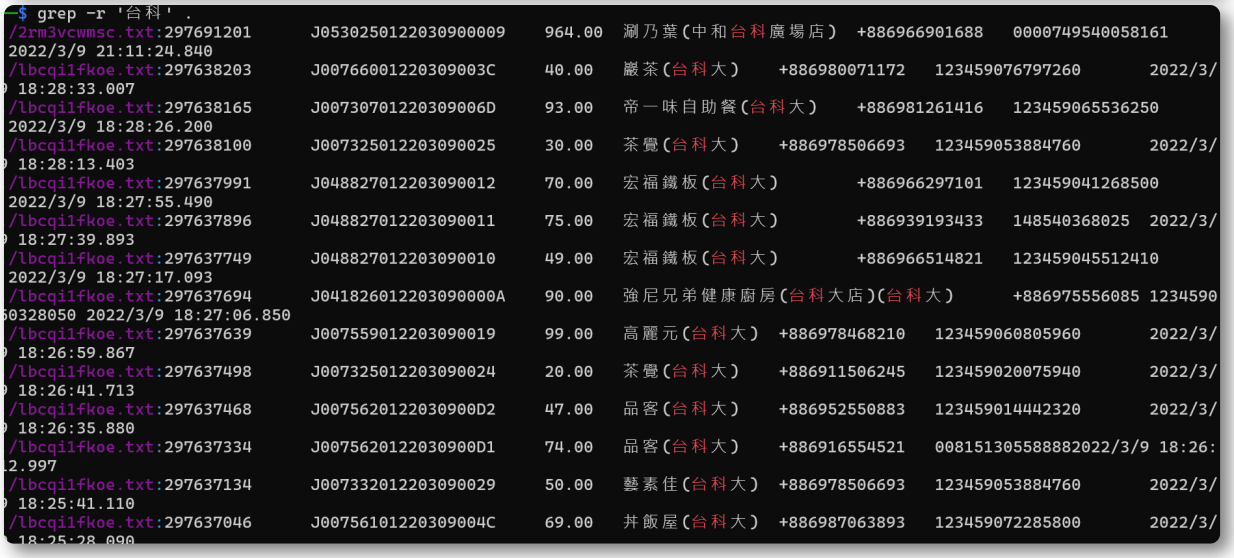
臺灣街口支付外洩資料

- URL：https://textbin.net/search?keyword=taiwan
- Date：Nov 4th, 2025
- Why it’s interesting?
  - Is old data but hot recently.

街口個資外洩引發疑慮 連資通安全署都被冒名行詐

郭 嘉
2025年10月13日

行動支付業者《街口支付》（JKOPay）近日遭爆料疑似外洩600萬筆用戶個資，包括用戶的ID、手機門號、身分證照片及銀行資料等機敏資訊都流到暗網，其中甚至涉及多位網紅與藝人個資；對此《街口支付》強調所有機敏資料皆採取進階加密防護，難以被詐騙集團再次利用。但此事件仍然引發各界關注與質疑，憂心資安破口將帶來危害。



- Indicators extracted:
  - PURCHASENO
  - PAYAMOUNT
  - TARGETTITLE
  - PAYACCOUNT
  - TRANSACTIONTIMETIME
- Confidence: Mid
- Safety/legality check: ilegal

Study Kestrel analytics

Kestrel Analytics Summary

Analytic	Goal	Input	Logic (1-line)	Output	Best Use Case	Limits
Lateral Movement Detection	Find abnormal auth behavior	Auth logs (user/IP)	Cluster-based deviation flagging	Adds cluster IDs & status	AD logon lateral move detection	Needs baseline; misses non-auth moves
Suspicious Process Scoring	Rank processes by suspicion	Sysmon / EDR process data	Heuristic/ML assigns score	`x_suspicious_score` attr	Triage noisy endpoint proc logs	False positives for admin tools
Pin IP on Map (Visual)	Geofence external IPs	Netflow / DNS / EDR net logs	Geolocate IP and map visualize	Adds geo attrs + map output	Beacon / C2 IP triage	Only context; not detection
XFE Enrichment *(inferred)*	Domain/IP reputation lookup	Web/DNS telemetry	Query reputation API → score/tag	Risk/category fields	Fast web/URL triage	Needs good threat feed; FP if generic
Log4Shell Deobfuscation *(inferred)*	Extract CVE-2021-44228 exploit IOCs	Java logs w/ JNDI	Parse + decode LDAP/JNDI strings	IOC fields (URI, C2)	Java appsec incident response	Very specific, misses other TTP

> SUMMARY BY CHATGPT

- Data source:
  - Sysmon process creation logs (with command-line and parent/child relationship)
  - DNS lookup logs and network traffic logs (via Netflow or EDR network telemetry)

collected into a central index (e.g., Elasticsearch).

- Kestrel analytic applied:
  - Use `susp_proc_scoring` to score new process creations across endpoints
  - highlighting processes with high `x_suspiciousness`. Then for high-scoring processes
  - use `pin_ip_on_map` to visualize outbound network traffic from those processes that reach external IP addresses
  - optionally `xfe_enrichment` on domains resolved by those processes.

- Enriched fields/IOCs:
  - For a process entity flagged by scoring, you would now have attributes like `x_suspiciousness` (from scoring), external destination IP(s), geolocation details for those IPs (from pin_map), domain reputation/risk attributes (from enrichment).
  - might also extract potential IOC domains/IPs from command-line.

- Follow-up hunt/detection:
    - Filter for processes where `x_suspiciousness` > threshold and dst_geo_country is outside your normal region and domain reputation risk score > certain level.
    - Then pivot to investigate:
        - on the endpoint
        - retrieve full command-line history
        - parent process chain
        - any loaded modules
    - in network logs, extract all traffic for that process's endpoint in the past 24h; in DNS logs, look for other domain resolutions by that endpoint. Tag as potential compromise if process executed unusual tool, connected to external suspicious domain, and spawned child processes or network activity.
    - Create detection rule in EDR/SIEM: if future process event scores above threshold and makes external connection with reputation risk > X → generate alert.