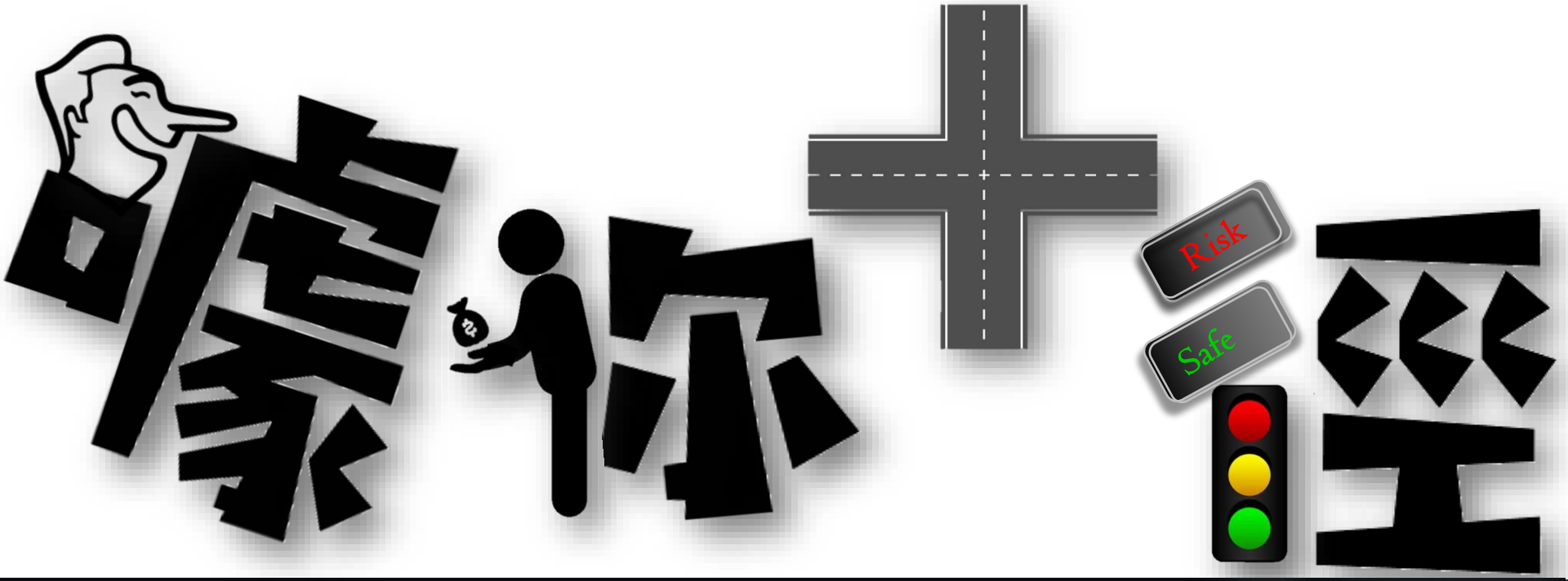
MJIB

# 資通安全與機密維護




2018/07/03 臺南市調查處資安科 李岱珊 (06) 298-7777 #185

# 十大噱頭

## SQL Injection


## 程式漏洞攻擊


## XSS 攻擊


## Wifi hacking


## Clickjacking


## CSRF跨站攻擊


## DDoS


## Ransomeware


## Phishing 釣魚


## Fraud 詐騙

[X] NEW ATTACK: FROM [PORTUGAL] TO [INDIA]
[X] NEW ATTACK: FROM [THAILAND] TO [DENMARK]
[X] NEW ATTACK: FROM [RUSSIAN FEDERATION] TO [UNITED STATES]
[X] NEW ATTACK: FROM [THAILAND] TO [MALAYSIA]

LOCAL TIME
15:52:13

ATTACKS TODAY
482,695

# FIREEYE CYBER THREAT MAP


ATTACKERS
TOP COUNTRIES
(PAST 30 DAYS)

Powered by FireEye Labs

TOP 5 REPORTED INDUSTRIES (PAST 30 DAYS)

- FINANCIAL SERVICES
- SERVICES/CONSULTING
- TELECOM
- MANUFACTURING
- INSURANCE

VIEW FULL SCREEN

The "FireEye Cyber Threat Map" is based on a subset of real attack data, which is optimized for better visual presentation. Customer information has been removed for privacy.

FireEye - Cyber Threat Map

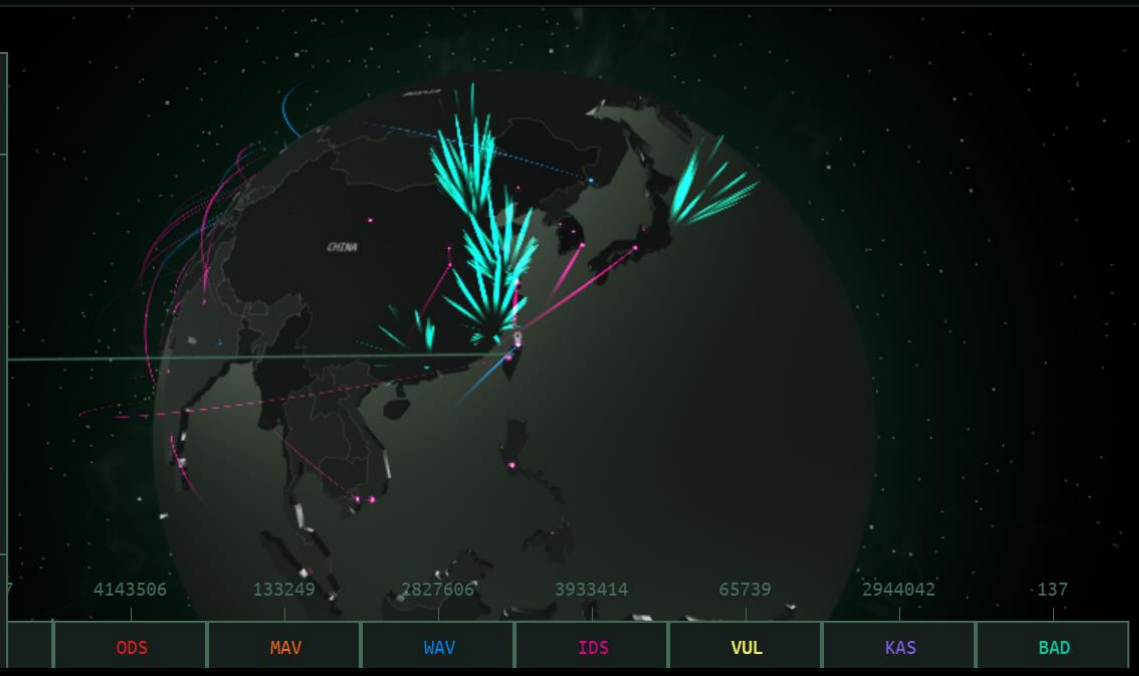
# CYBERTHREAT REAL-TIME MAP

EN

Download Trial

MAP STATISTICS DATA SOURCES BUZZ WIDGET

Share




## TAIWAN

# 13 MOST-ATTACKED COUNTRY

| | |
|---|---|
| OAS | 48938 |
| ODS | 51144 |
| MAV | 6673 |
| WAV | 50476 |
| IDS | 173265 |
| VUL | 787 |
| KAS | 8481 |
| BAD | 0 |

Detections discovered since 00:00 GMT

More details

Share data

DEMO ON

Kaspersky - Cyberthreat Real-Time Map

# CYBERTHREAT REAL-TIME MAP

EN

Download Trial

MAP | STATISTICS | DATA SOURCES | BUZZ | WIDGET

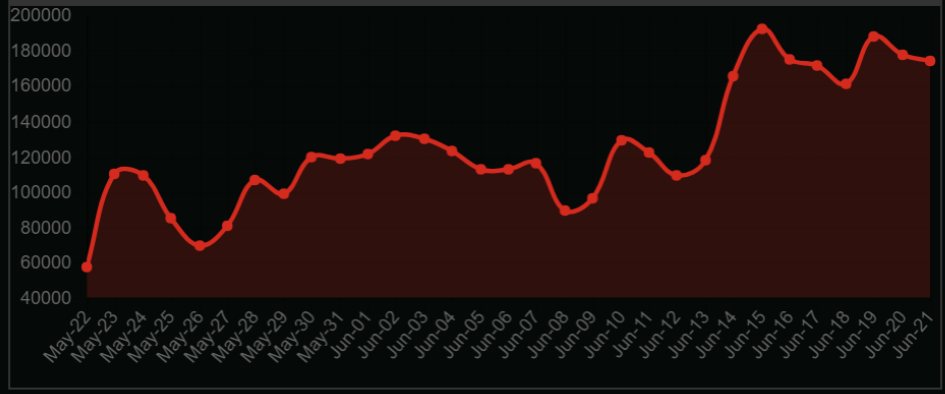
Share

HISTORICAL STATISTICS

## PER COUNTRY

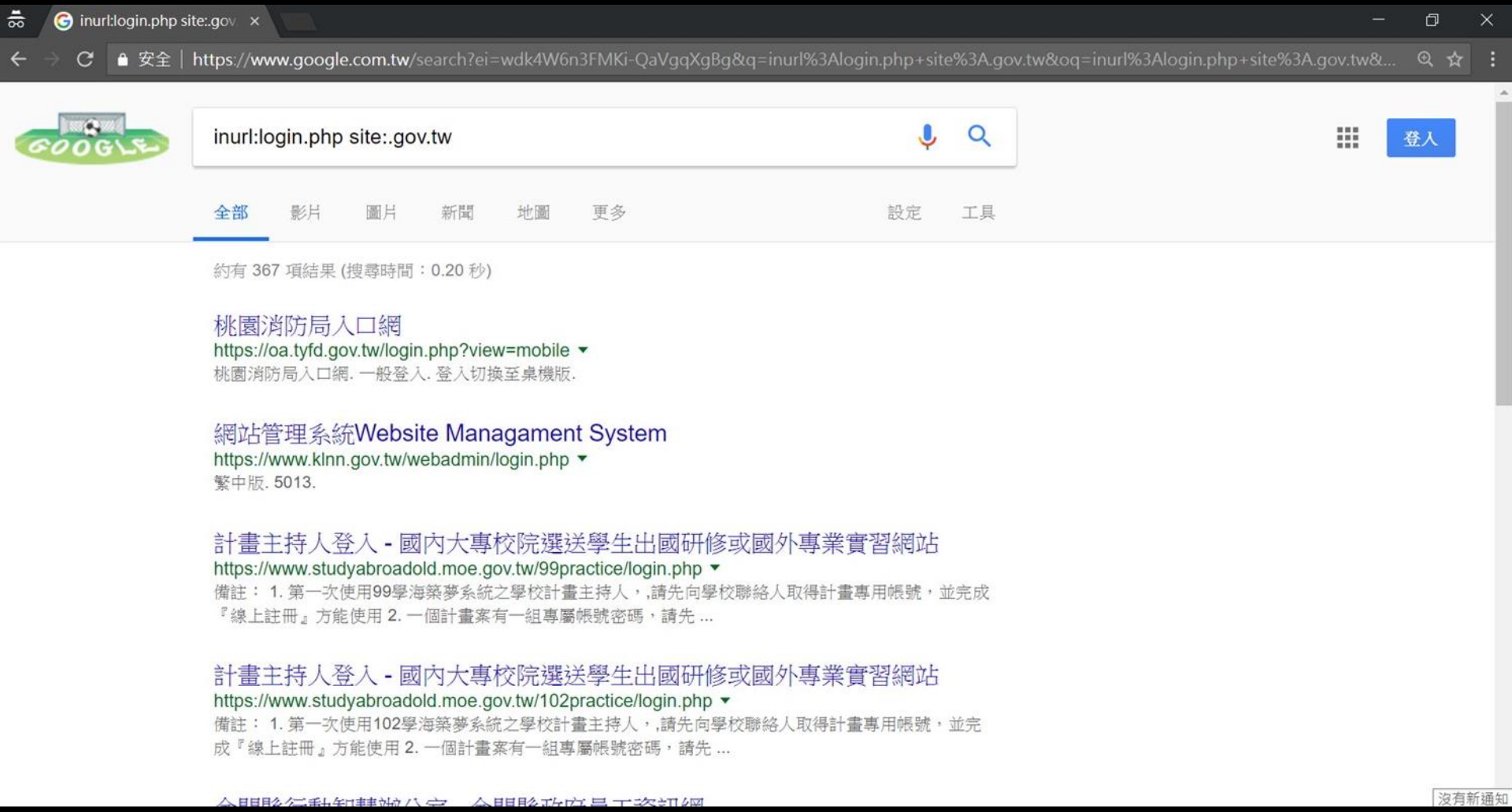
Taiwan | Web threats | TIME PERIOD: Last week | Last month

### Top - Web threats IN THE LAST MONTH

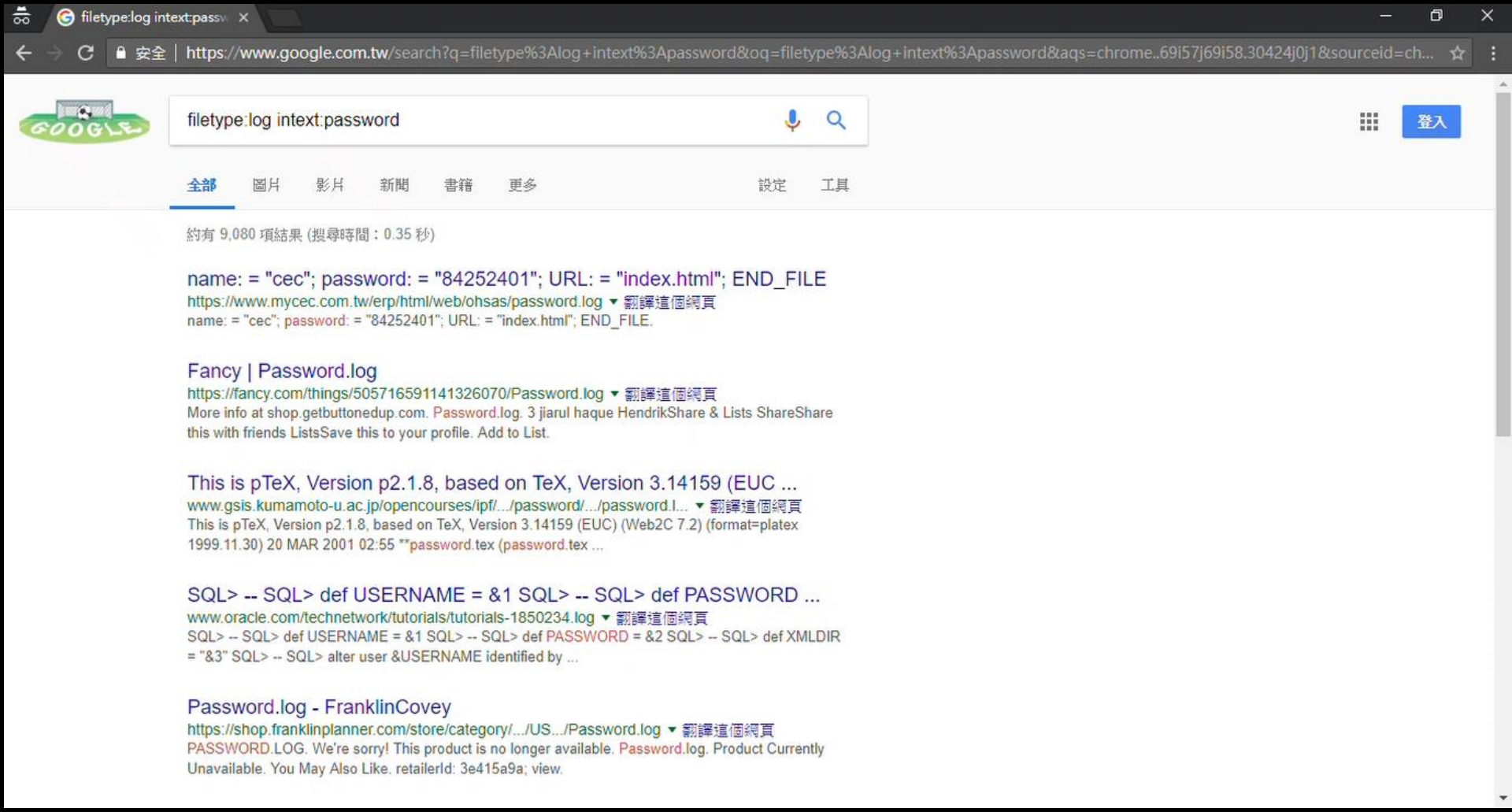



### Top - Web threats IN THE LAST MONTH

| | | |
|---|---|---|
| 1 | Trojan.Script.Miner.gen | 15.2% |
| 2 | Exploit.Win32.CVE-2017-11882.gen | 12.4% |
| 3 | Trojan-Clicker.HTML.Iframe.dg | 9.6% |
| 4 | Trojan.Script.Generic | 9.5% |
| 5 | Packed.Multi.MultiPacked.gen | 7.14% |
| 6 | Trojan.PDF.Phish.wr | 4.83% |
| 7 | Trojan-Downloader.MSOffice.Agent.sb | 4.1% |
| 8 | Trojan-Downloader.JS.SLoad.gen | 4.01% |
| 9 | Trojan-Downloader.VBS.Agent.clp | 3.97% |
| 10 | Trojan-Dropper.VBS.Agent.bp | 3.86% |


inurl:login.php site:.gov
安全 | https://www.google.com.tw/search?ei=wdk4W6n3FMKi-QaVgqXgBg&q=inurl%3Alogin.php+site%3A.gov.tw&oq=inurl%3Alogin.php+site%3A.gov.tw&...
inurl:login.php site:.gov.tw
登入
全部 影片 圖片 新聞 地圖 更多 設定 工具
約有 367 項結果 (搜尋時間：0.20 秒)
桃園消防局入口網
https://oa.tyfd.gov.tw/login.php?view=mobile
桃園消防局入口網. 一般登入. 登入切換至桌機版.
網站管理系統Website Managament System
https://www.klnn.gov.tw/webadmin/login.php
繁中版. 5013.
計畫主持人登入 - 國內大專校院選送學生出國研修或國外專業實習網站
https://www.studyabroadold.moe.gov.tw/99practice/login.php
備註： 1. 第一次使用99學海築夢系統之學校計畫主持人，,請先向學校聯絡人取得計畫專用帳號，並完成『線上註冊』方能使用 2. 一個計畫案有一組專屬帳號密碼，請先 ...
計畫主持人登入 - 國內大專校院選送學生出國研修或國外專業實習網站
https://www.studyabroadold.moe.gov.tw/102practice/login.php
備註： 1. 第一次使用102學海築夢系統之學校計畫主持人，,請先向學校聯絡人取得計畫專用帳號，並完成『線上註冊』方能使用 2. 一個計畫案有一組專屬帳號密碼，請先 ...
沒有新通知


inurl:admin.php site:.go
安全 | https://www.google.com.tw/search?q=inurl%3Aadmin.php+site%3A.gov.tw&oq=inurl%3Aadmin.php+site%3A.gov.tw&aqs=chrome..69i57j69i58.4084j0j...
inurl:admin.php site:.gov.tw
登入
全部 圖片 新聞 影片 地圖 更多 設定 工具
9 項結果 (搜尋時間：0.17 秒)
臺灣省台東農田水利會-網站管理系統
www.ttia.gov.tw/admin.php
會址：台東市新生路190號服務電話：(089)326100-2 No.190, Sinsheng Rd., Taitung City, Taitung County 950, Taiwan (R.O.C.). 最佳瀏覽1024*768 All Rights ...
管理介面 - 台灣原住民知識社群
blog.tacp.gov.tw/admin.php
登入. 歡迎使用台灣原住民族知識社群管理平台！ 使用者名稱. 使用者密碼. 忘記密碼? 回到首頁.
桃園眷村鐵三角網站- 後端管理系統
tynewvillage.tyccc.gov.tw/admin/admin.php
登出.
管理者登入 - 資訊志工 - 教育部
https://ecare.moe.gov.tw/ecare/admin.php
106年度教育部資訊志工計畫』. 管理者帳號：. 管理者密碼：. 輸入下列驗證碼：. 資訊志工營運中心.
國家重要濕地資料庫入口網站管理系統 - 國家重要濕地保育計畫


filetype:log intext:passv
安全 | https://www.google.com.tw/search?q=filetype%3Alog+intext%3Apassword&oq=filetype%3Alog+intext%3Apassword&aqs=chrome..69i57j69i58.30424j0j1&sourceid=ch...
filetype:log intext:password
登入
全部 圖片 影片 新聞 書籍 更多 設定 工具
約有 9,080 項結果 (搜尋時間：0.35 秒)
name: = "cec"; password: = "84252401"; URL: = "index.html"; END_FILE
https://www.mycec.com.tw/erp/html/web/ohsas/password.log ▾ 翻譯這個網頁
name: = "cec"; password: = "84252401"; URL: = "index.html"; END_FILE.
Fancy | Password.log
https://fancy.com/things/505716591141326070/Password.log ▾ 翻譯這個網頁
More info at shop.getbuttonedup.com. Password.log. 3 jiarul haque HendrikShare & Lists ShareShare this with friends ListsSave this to your profile. Add to List.
This is pTeX, Version p2.1.8, based on TeX, Version 3.14159 (EUC ...
www.gsis.kumamoto-u.ac.jp/opencourses/ipf/.../password/.../password.l... ▾ 翻譯這個網頁
This is pTeX, Version p2.1.8, based on TeX, Version 3.14159 (EUC) (Web2C 7.2) (format=platex 1999.11.30) 20 MAR 2001 02:55 **password.tex (password.tex ...
SQL> -- SQL> def USERNAME = &1 SQL> -- SQL> def PASSWORD ...
www.oracle.com/technetwork/tutorials/tutorials-1850234.log ▾ 翻譯這個網頁
SQL> -- SQL> def USERNAME = &1 SQL> -- SQL> def PASSWORD = &2 SQL> -- SQL> def XMLDIR = "&3" SQL> -- SQL> alter user &USERNAME identified by ...
Password.log - FranklinCovey
https://shop.franklinplanner.com/store/category/.../US.../Password.log ▾ 翻譯這個網頁
PASSWORD.LOG. We're sorry! This product is no longer available. Password.log. Product Currently Unavailable. You May Also Like. retailerId: 3e415a9a; view.

# 兩條路徑

**SQL Injection**


**程式漏洞攻擊**


**XSS 攻擊**


**Wifi hacking**


## 社交工程

**Clickjacking**


**CSRF跨站攻擊**


**DDoS**

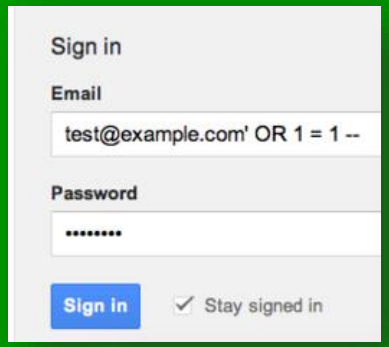

## 漏洞攻擊

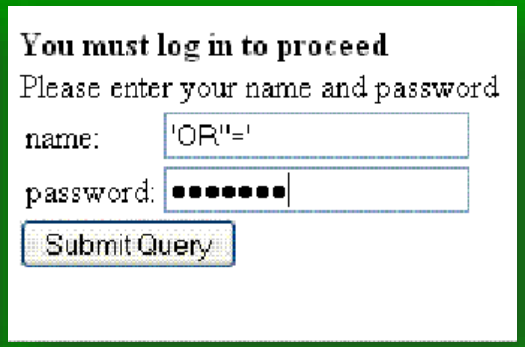
**Ransomeware**

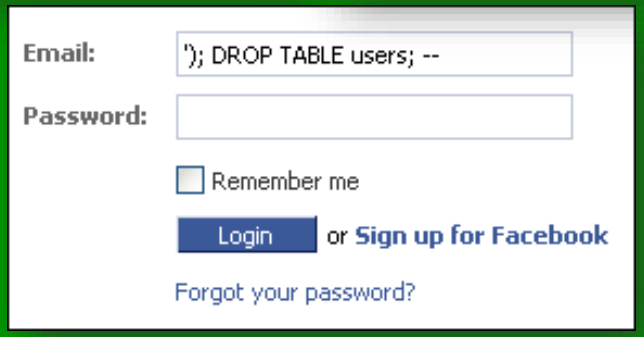

**Phishing 釣魚**


**Fraud 詐騙**

## SQL Injection

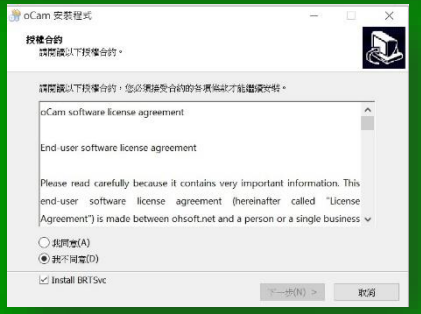



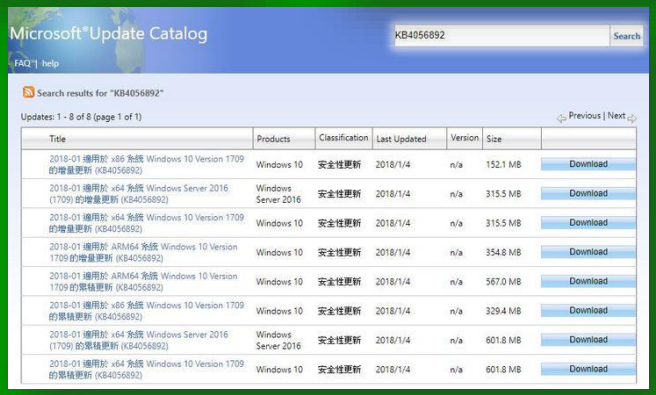




## 程式漏洞攻擊



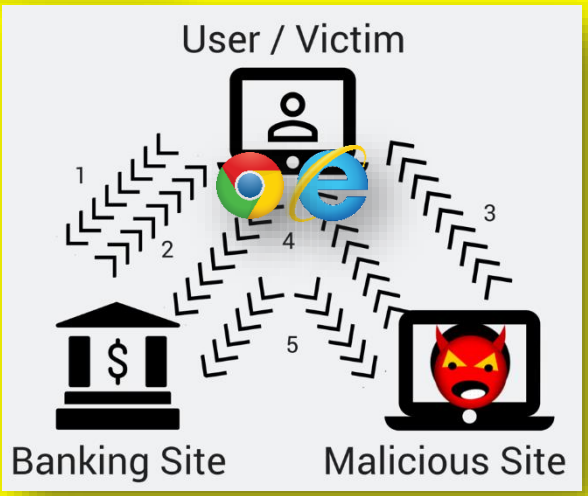


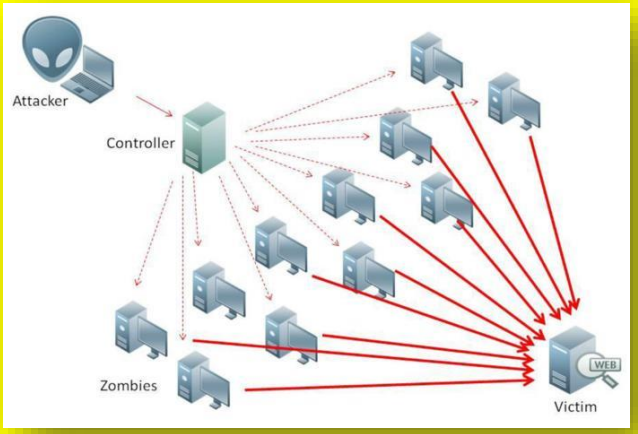
## Clickjacking



## CSRF跨站攻擊


## DDoS

## XSS 攻擊



```
<html>
    <head>

    </head>
    <body>
        <script>
            var user_comment = get_user_last_comment();
            var comment = document.getElementById("comment");
            comment.innerHTML = comment;
        </script>
        <div id="comment">
    </body>
</html>
```

iframe

XSS

## Wifi hacking



連上去個資全露
EBC東森新聞HD
公共WiFi
個資恐遭駭
你也是這樣
獨家
EXCLUSIVE
EXCLUSIVE
EXCLUSIVE

## Ransomeware



## Phishing 釣魚



## Fraud 詐騙



"+1遭詐!"看直播下單購物 卻收到詐騙帳號

CBC NEWS | 下載APP看直播 |

# 五大損害

破壞性

盜用身分

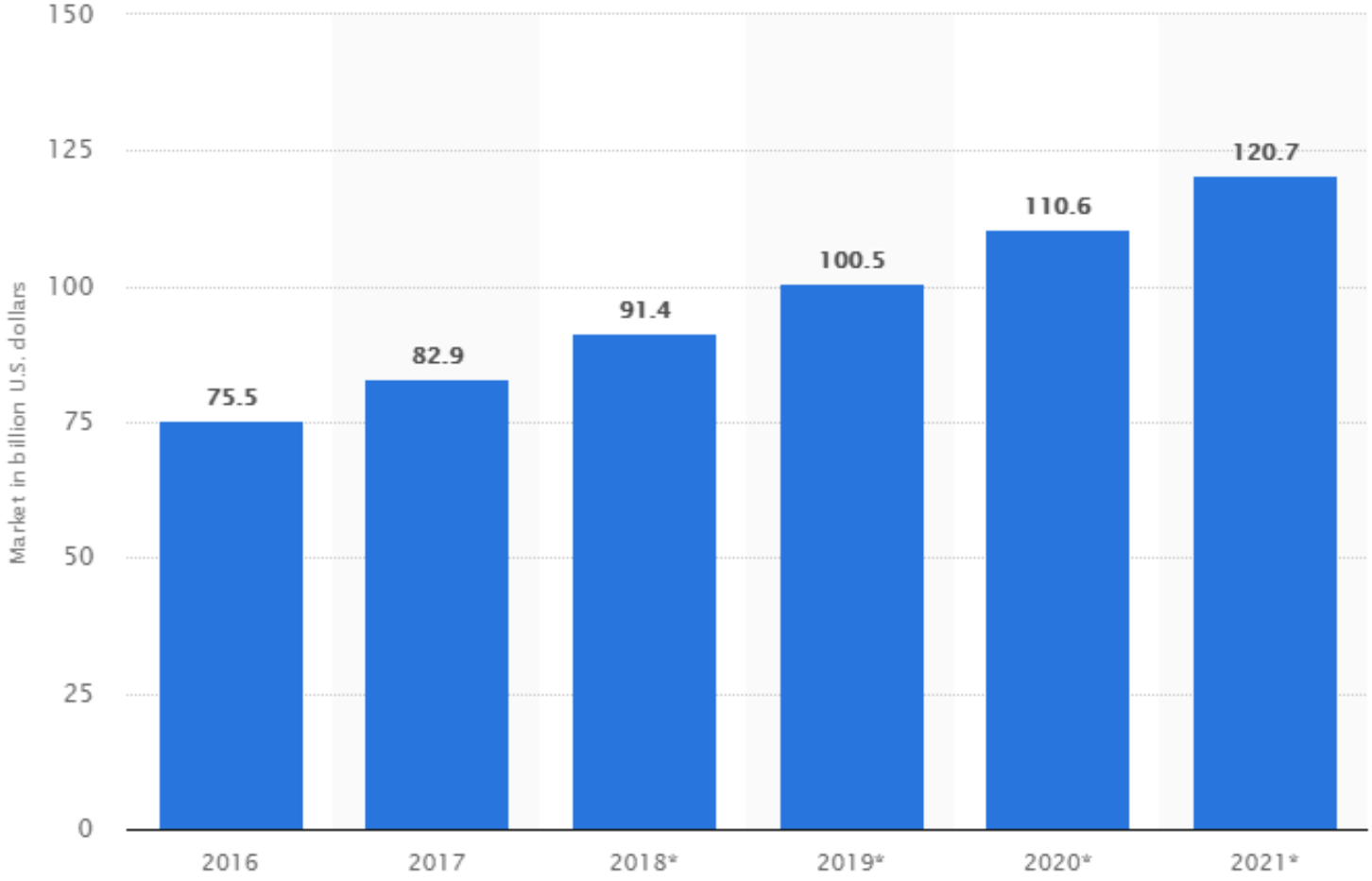
金融詐欺

竊取資料


濫用資源

# 資安防護商機

***2016-2021 Size of the information security technology market (in billion U.S. dollars)***




https://www.statista.com/statistics/640141/worldwide-information-security-market-size/

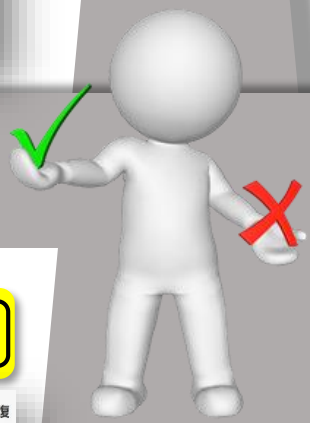
# 安心上路？

**SQL Injection**


**程式漏洞攻擊**


**XSS 攻擊**


**Wifi hacking**

## 社交工程

**Clickjacking**


**CSRF跨站攻擊**


**DDoS**


## 漏洞攻擊

**Ransomeware**

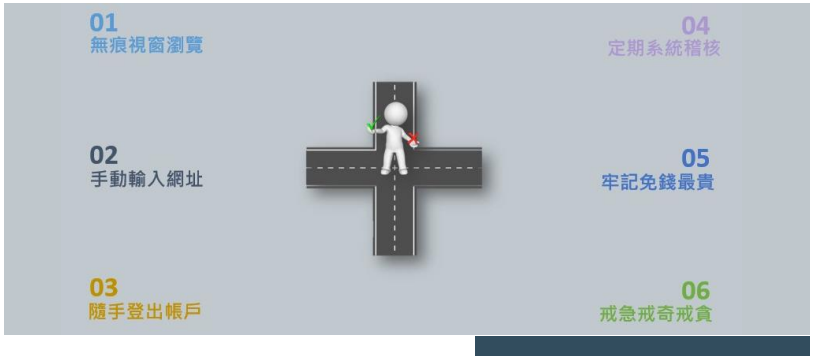

**Phishing 釣魚**


**Fraud 詐騙**

# 網路如唬口，留神小心走

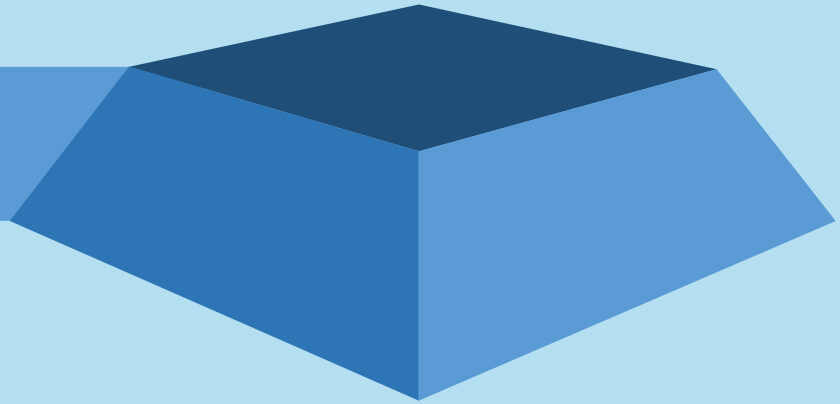


事前防範 → 過程保護 → 證據留存 → 通報追查




# 事前防範

## 基礎防護



**內外隔離**

個人電腦應安裝防毒軟體，並隔離外部及內部網路、分別訂定安全層級，另落實系統存取之權限控制

# 事前防範


**弱點掃瞄**

即時更新作業系統及應用程式之修補程式、使用者帳號密碼應定期更新，且不得使用不安全密碼

**內外隔離**

個人電腦應安裝防毒軟體，並隔離外部及內部網路、分別訂定安全層級，另落實系統存取之權限控制

# 事前防範

**加強宣導**

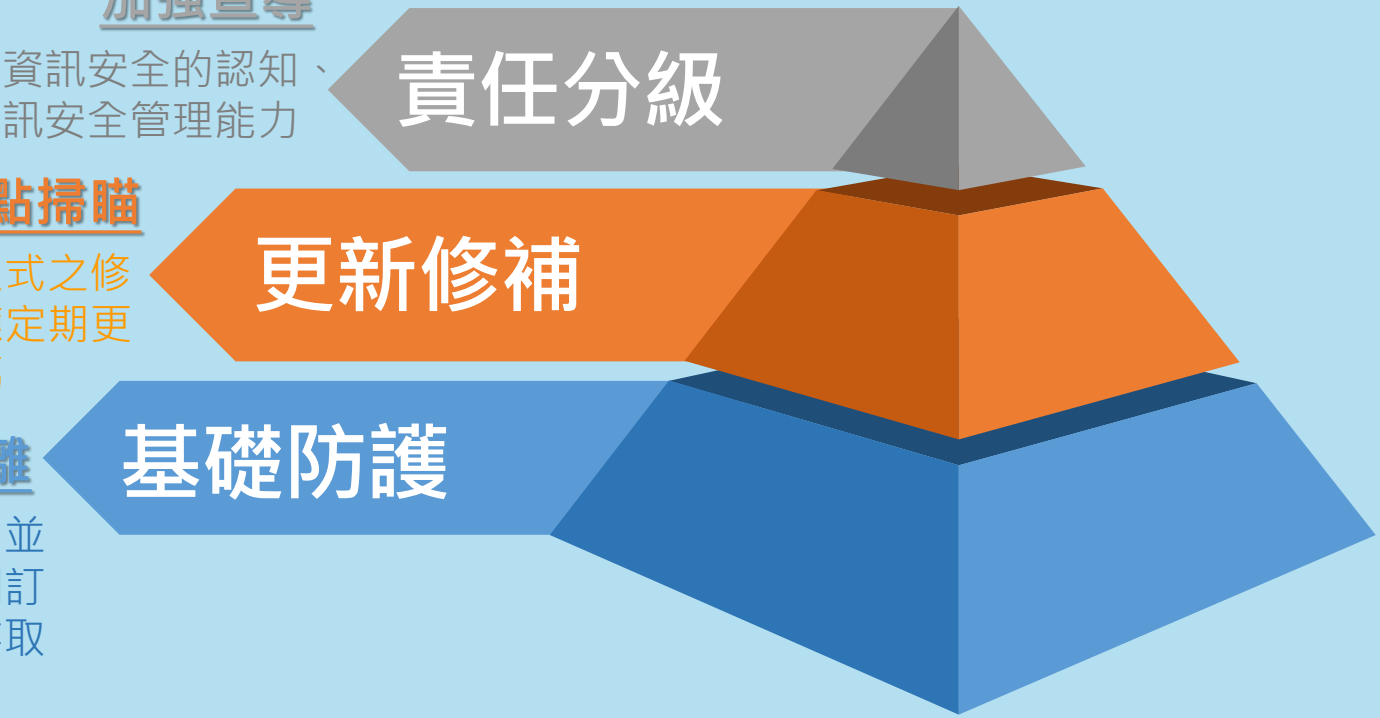
加強宣導一般人員對資訊安全的認知、提升系統管理人員資訊安全管理能力

**弱點掃瞄**

即時更新作業系統及應用程式之修補程式、使用者帳號密碼應定期更新，且不得使用不安全密碼

**內外隔離**

個人電腦應安裝防毒軟體，並隔離外部及內部網路、分別訂定安全層級，另落實系統存取之權限控制

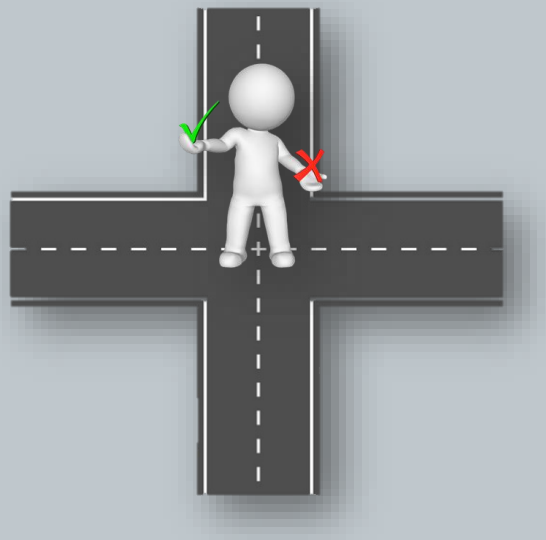


# 過程保護

01
無痕視窗瀏覽

02
手動輸入網址

03
隨手登出帳戶



04
定期系統稽核

05
牢記免錢最貴

06
戒急戒奇戒貪

# 過程保護

**01**
**無痕視窗瀏覽**

**02**
**手動輸入網址**

**03**
**隨手登出帳戶**

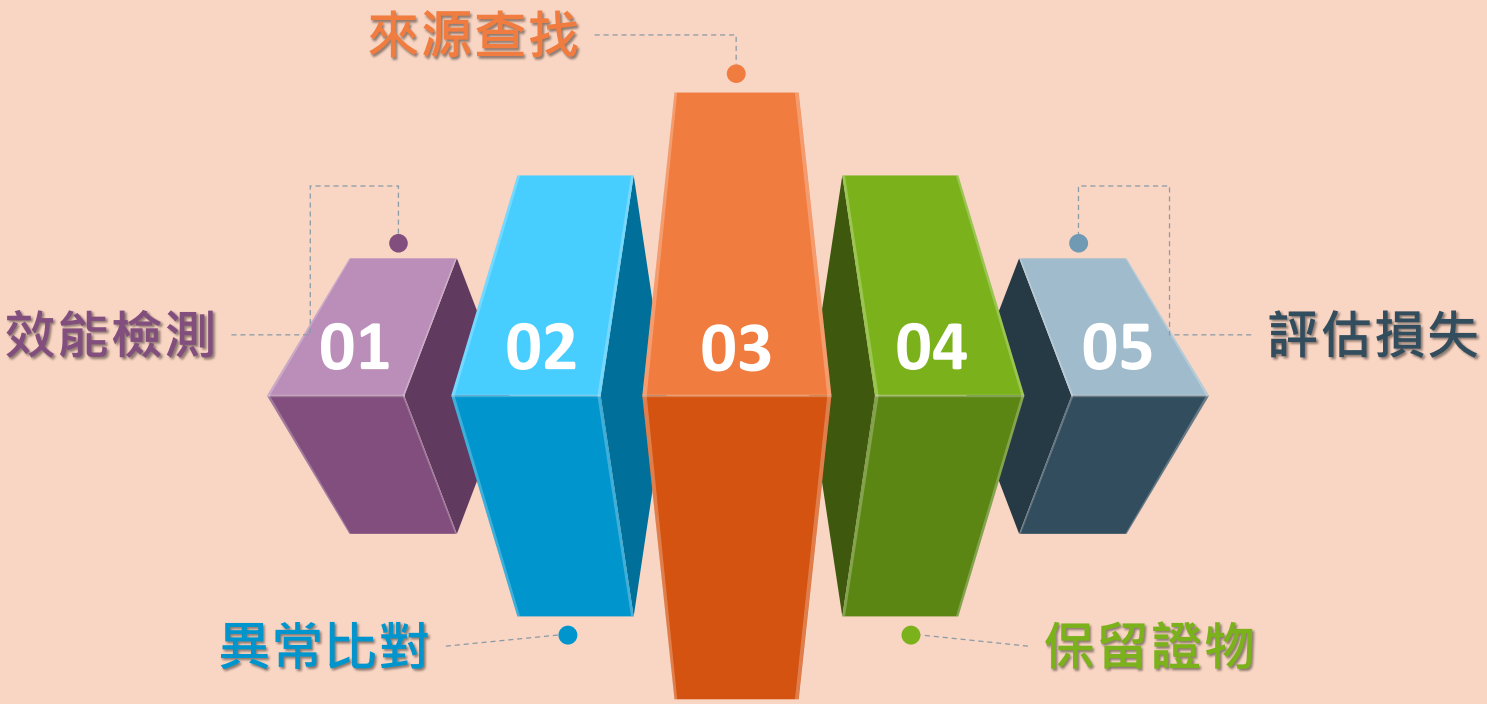
# 過程保護

04
定期系統稽核

05
牢記免錢最貴

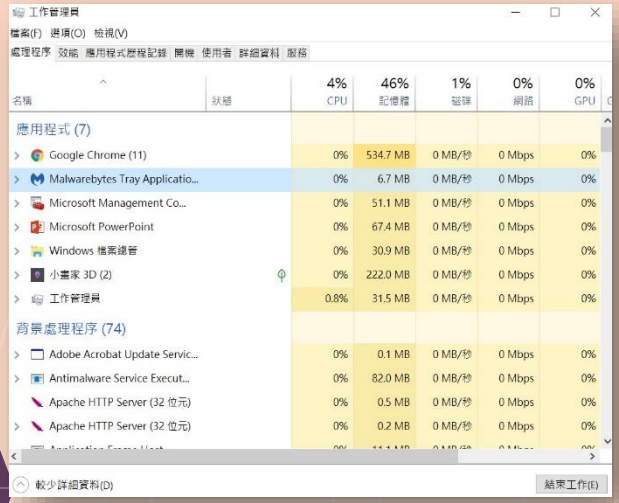
06
戒急戒奇戒貪

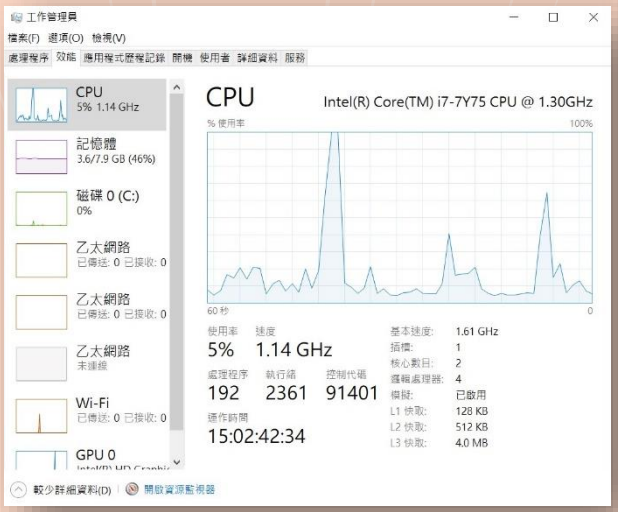
# 證據留存



# 證據留存

效能檢測 01


工作管理員
檔案(F) 選項(O) 檢視(V)
處理程序 效能 應用程式歷程記錄 開機 使用者 詳細資料 服務
名稱 狀態 4% CPU 46% 記憶體 1% 磁碟 0% 網路 0% GPU
應用程式 (7)
Google Chrome (11) 0% 534.7 MB 0 MB/秒 0 Mbps 0%
Malwarebytes Tray Applicatio... 0% 6.7 MB 0 MB/秒 0 Mbps 0%
Microsoft Management Co... 0% 51.1 MB 0 MB/秒 0 Mbps 0%
Microsoft PowerPoint 0% 67.4 MB 0 MB/秒 0 Mbps 0%
Windows 檔案總管 0% 30.9 MB 0 MB/秒 0 Mbps 0%
小畫家 3D (2) 0% 222.0 MB 0 MB/秒 0 Mbps 0%
工作管理員 0.8% 31.5 MB 0 MB/秒 0 Mbps 0%
背景處理程序 (74)
Adobe Acrobat Update Servic... 0% 0.1 MB 0 MB/秒 0 Mbps 0%
Antimalware Service Execut... 0% 82.0 MB 0 MB/秒 0 Mbps 0%
Apache HTTP Server (32 位元) 0% 0.5 MB 0 MB/秒 0 Mbps 0%
Apache HTTP Server (32 位元) 0% 0.2 MB 0 MB/秒 0 Mbps 0%
較少詳細資料(D)
結束工作(E)


工作管理員
檔案(F) 選項(O) 檢視(V)
處理程序 效能 應用程式歷程記錄 開機 使用者 詳細資料 服務
CPU
5% 1.14 GHz
記憶體
3.6/7.9 GB (46%)
磁碟 0 (C:)
0%
乙太網路
已傳送: 0 已接收: 0
乙太網路
已傳送: 0 已接收: 0
乙太網路
未連線
Wi-Fi
已傳送: 0 已接收: 0
GPU 0
CPU
Intel(R) Core(TM) i7-7Y75 CPU @ 1.30GHz
% 使用率
100%
60 秒
0
使用率
5%
速度
1.14 GHz
處理程序
192
執行緒
2361
控制代碼
91401
通作時間
15:02:42:34
基本速度: 1.61 GHz
插槽: 1
核心數目: 2
邏輯處理器: 4
模擬: 已啟用
L1 快取: 128 KB
L2 快取: 512 KB
L3 快取: 4.0 MB
較少詳細資料(D)
開啟資源監視器

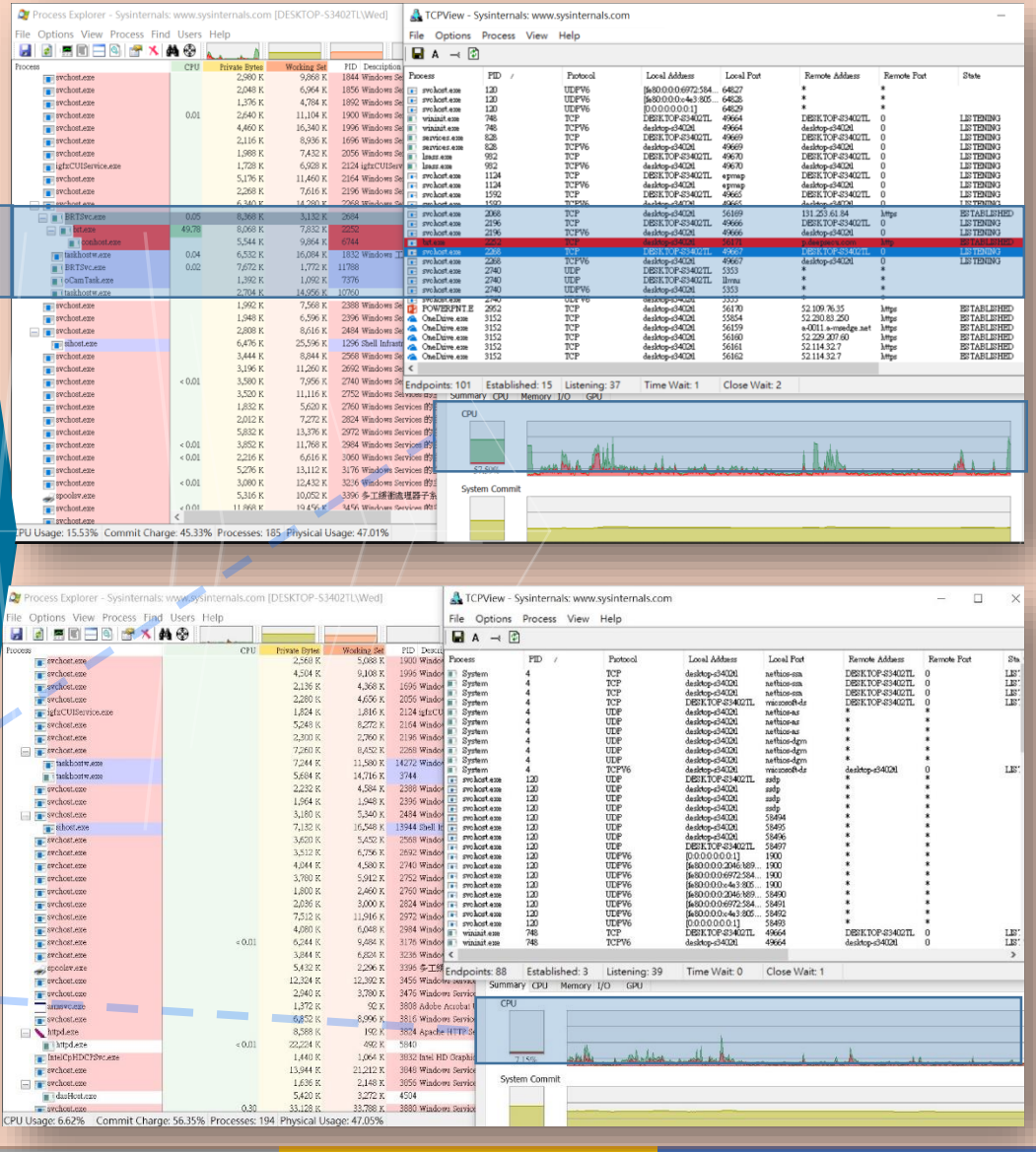

遠傳電信 4G
下午6:49
100%
個人熱點：1 個連線
設定
電池
電池用量
過去 24 小時
過去 7 天
LINE 32%
Safari 21%
照片 20%
Between
背景活動 12%
相機
音訊 5%
Siri 4%
主畫面與鎖定畫面 3%
麥當勞報報 2%
時鐘 1%
顯示過去 24 小時每個 App 使用的電池比例。
自上次完全充電以來的使用時間

# 證據留存

出現作用不明的程式

異常比對

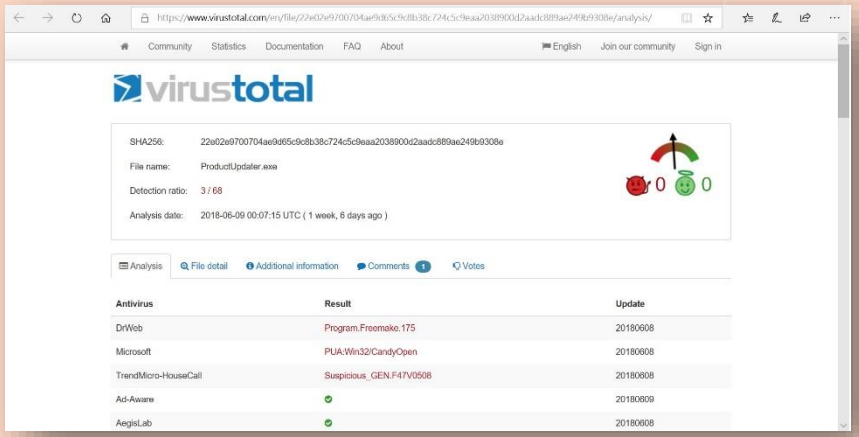
突然飆升的用量



# 證據留存

來源查找

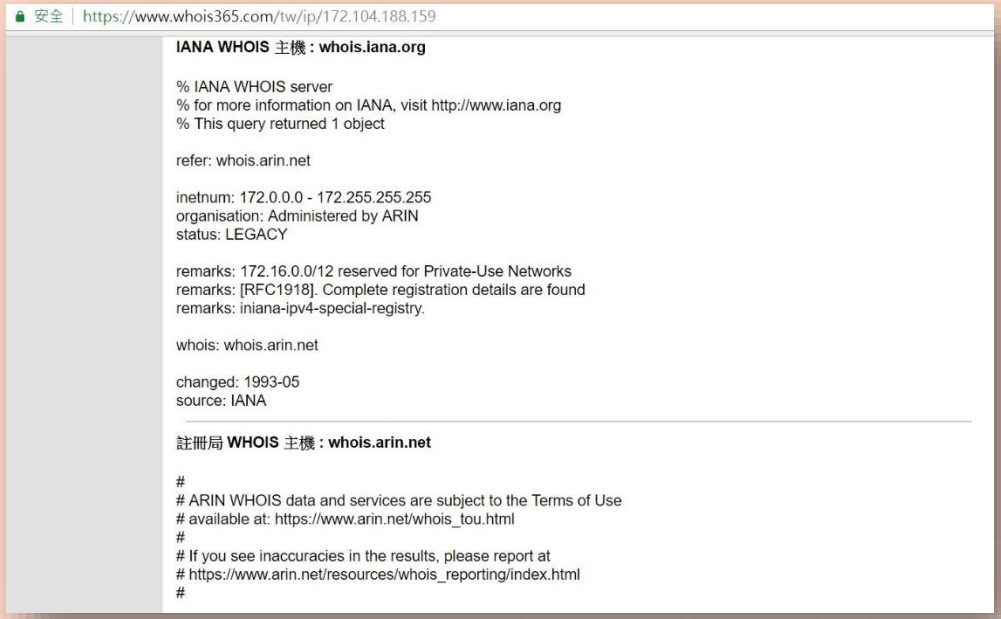
03


virustotal
SHA256: 22e02e9700704ae9d65c9c8b38c724c5c9eaa2038900d2aadc889ae249b9308e
File name: ProductUpdater.exe
Detection ratio: 3 / 68
Analysis date: 2018-06-09 00:07:15 UTC ( 1 week, 6 days ago )
Analysis
File detail
Additional information
Comments
Votes
Antivirus
Result
Update
DrWeb
Program.Freemake.175
20180608
Microsoft
PUA:Win32/CandyOpen
20180608
TrendMicro-HouseCall
Suspicious_GEN.F47V0508
20180608
Ad-Aware
20180609
AegisLab
20180608


安全 | https://www.whois365.com/tw/about
請輸入網域名稱或 IP 位址
查詢
說明
關於 全球 WHOIS 查詢
全球 WHOIS 查詢 是一個用於查詢以下項目的網頁 WHOIS 查詢工具：
網域名稱 WHOIS 查詢
國際頂級網域 (gTLD)
.com .net .org .biz .info 及更多。
新的國際頂級網域 (gTLD)
.accountants .house .ninja .world 及更多。
國家及地區頂級網域 (ccTLD)
.cc .tv .jp .cn .hk .tw .de 及更多。
支援 IDN (國際化網域名稱)
IDN.com, IDN.tw, IDN.中国 及更多。
全球 WHOIS 查詢 目前支援 734 種 gTLD 及 ccTLD 網域的查詢。
IP 位址 WHOIS 查詢
IPv4 位址
IPv4 位址、十進位 IP 位址。
IPv6 位址
IPv6 位址, 縮短的 IPv6 位址亦可。


安全 | https://whois.tanet.edu.tw
資訊及科技教育司
TANet Whois Database
IP Whois 查詢：
送出
重設
連絡我們

# 證據留存


安全 | https://www.whois365.com/tw/ip/172.104.188.159

**IANA WHOIS 主機 : whois.iana.org**

% IANA WHOIS server
% for more information on IANA, visit http://www.iana.org
% This query returned 1 object

refer: whois.arin.net

inetnum: 172.0.0.0 - 172.255.255.255
organisation: Administered by ARIN
status: LEGACY

remarks: 172.16.0.0/12 reserved for Private-Use Networks
remarks: [RFC1918]. Complete registration details are found
remarks: iniana-ipv4-special-registry.

whois: whois.arin.net

changed: 1993-05
source: IANA

---

**註冊局 WHOIS 主機 : whois.arin.net**

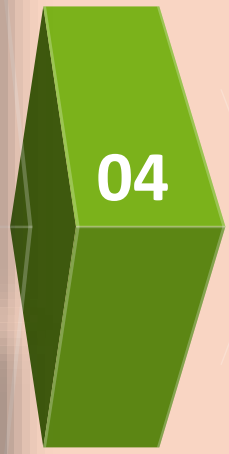
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/whois_reporting/index.html
#


cports.log - 記事本

檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 2018/6/22 下午 02:03:11 | Removed | 0 | Unknown | TCP | 192.168.1.22:56665 | 52.239.177.100:443 | |
| 2018/6/22 下午 02:03:21 | Added | 12212 | chrome.exe | UDP | 0.0.0.0:53687 | | DESKTOP-S3402TL\Wed |
| 2018/6/22 下午 02:03:21 | Added | 12212 | chrome.exe | UDP | 0.0.0.0:53688 | | DESKTOP-S3402TL\Wed |
| 2018/6/22 下午 02:03:21 | Added | 2740 | svchost.exe | UDP | 0.0.0.0:53686 | | |
| 2018/6/22 下午 02:03:21 | Added | 2740 | svchost.exe | UDP | [::]:53686 | | |
| 2018/6/22 下午 02:03:23 | Removed | 2740 | svchost.exe | UDP | 0.0.0.0:53686 | | |
| 2018/6/22 下午 02:03:23 | Removed | 2740 | svchost.exe | UDP | [::]:53686 | | |
| 2018/6/22 下午 02:03:27 | Added | 12212 | chrome.exe | UDP | 0.0.0.0:64201 | | DESKTOP-S3402TL\Wed |
| 2018/6/22 下午 02:03:35 | Added | 6572 | MBAMService.exe | TCP | 192.168.1.22:56677 | 52.0.161.176:443 | |
| 2018/6/22 下午 02:03:37 | Removed | 6572 | MBAMService.exe | TCP | 192.168.1.22:56677 | 52.0.161.176:443 | |
| 2018/6/22 下午 02:03:43 | Removed | 1064 | svchost.exe | TCP | 192.168.1.22:56669 | 118.214.247.47:443 | |
| 2018/6/22 下午 02:03:55 | Added | 12212 | chrome.exe | UDP | 192.168.6.1:51728 | | DESKTOP-S3402TL\Wed |
| 2018/6/22 下午 02:03:55 | Added | 12212 | chrome.exe | UDP | 192.168.145.1:51729 | | DESKTOP-S3402TL\Wed |
| 2018/6/22 下午 02:03:55 | Added | 12212 | chrome.exe | UDP | 192.168.1.22:51730 | | DESKTOP-S3402TL\Wed |
| 2018/6/22 下午 02:03:59 | Removed | 12212 | chrome.exe | UDP | 192.168.6.1:51728 | | DESKTOP-S3402TL\Wed |
| 2018/6/22 下午 02:03:59 | Removed | 12212 | chrome.exe | UDP | 192.168.145.1:51729 | | DESKTOP-S3402TL\Wed |
| 2018/6/22 下午 02:03:59 | Removed | 12212 | chrome.exe | UDP | 192.168.1.22:51730 | | DESKTOP-S3402TL\Wed |
| 2018/6/22 下午 02:04:01 | Removed | 8260 | SearchUI.exe | TCP | 192.168.1.22:56674 | 13.107.49.254:443 | DESKTOP-S3402TL\Wed |
| 2018/6/22 下午 02:04:03 | Removed | 8260 | SearchUI.exe | TCP | 192.168.1.22:56672 | 204.79.197.254:443 | DESKTOP-S3402TL\Wed |
| 2018/6/22 下午 02:04:03 | Removed | 8260 | SearchUI.exe | TCP | 192.168.1.22:56675 | 204.79.197.222:443 | DESKTOP-S3402TL\Wed |

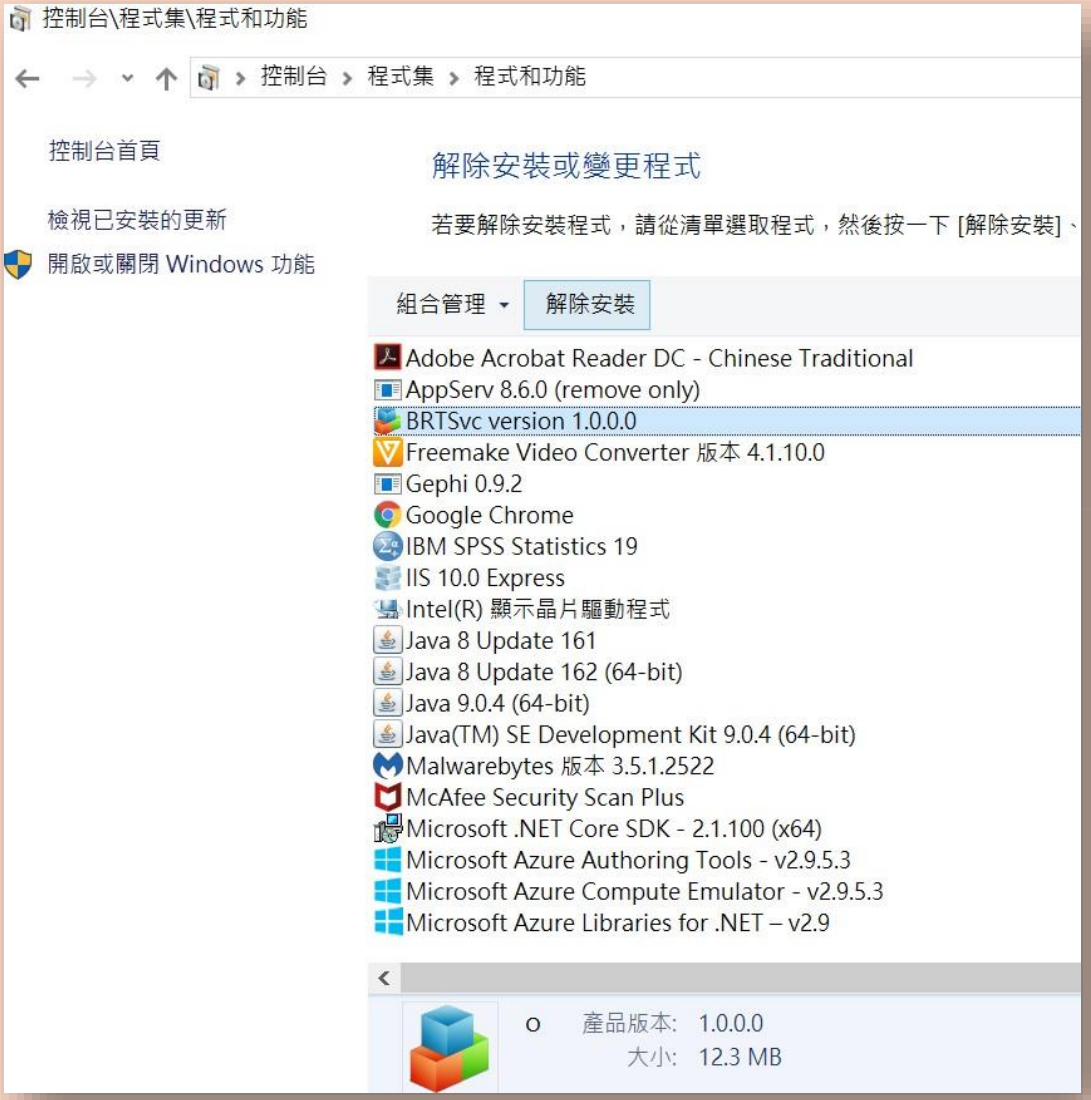
留存ip查詢結果

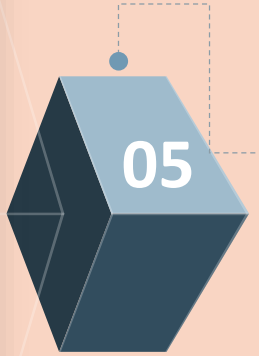



保留證物

留存log檔案

# 證據留存


控制台\程式集\程式和功能
控制台 › 程式集 › 程式和功能
控制台首頁
檢視已安裝的更新
開啟或關閉 Windows 功能
解除安裝或變更程式
若要解除安裝程式，請從清單選取程式，然後按一下 [解除安裝]、
組合管理
解除安裝
Adobe Acrobat Reader DC - Chinese Traditional
AppServ 8.6.0 (remove only)
BRTSvc version 1.0.0.0
Freemake Video Converter 版本 4.1.10.0
Gephi 0.9.2
Google Chrome
IBM SPSS Statistics 19
IIS 10.0 Express
Intel(R) 顯示晶片驅動程式
Java 8 Update 161
Java 8 Update 162 (64-bit)
Java 9.0.4 (64-bit)
Java(TM) SE Development Kit 9.0.4 (64-bit)
Malwarebytes 版本 3.5.1.2522
McAfee Security Scan Plus
Microsoft .NET Core SDK - 2.1.100 (x64)
Microsoft Azure Authoring Tools - v2.9.5.3
Microsoft Azure Compute Emulator - v2.9.5.3
Microsoft Azure Libraries for .NET – v2.9
產品版本: 1.0.0.0
大小: 12.3 MB


05

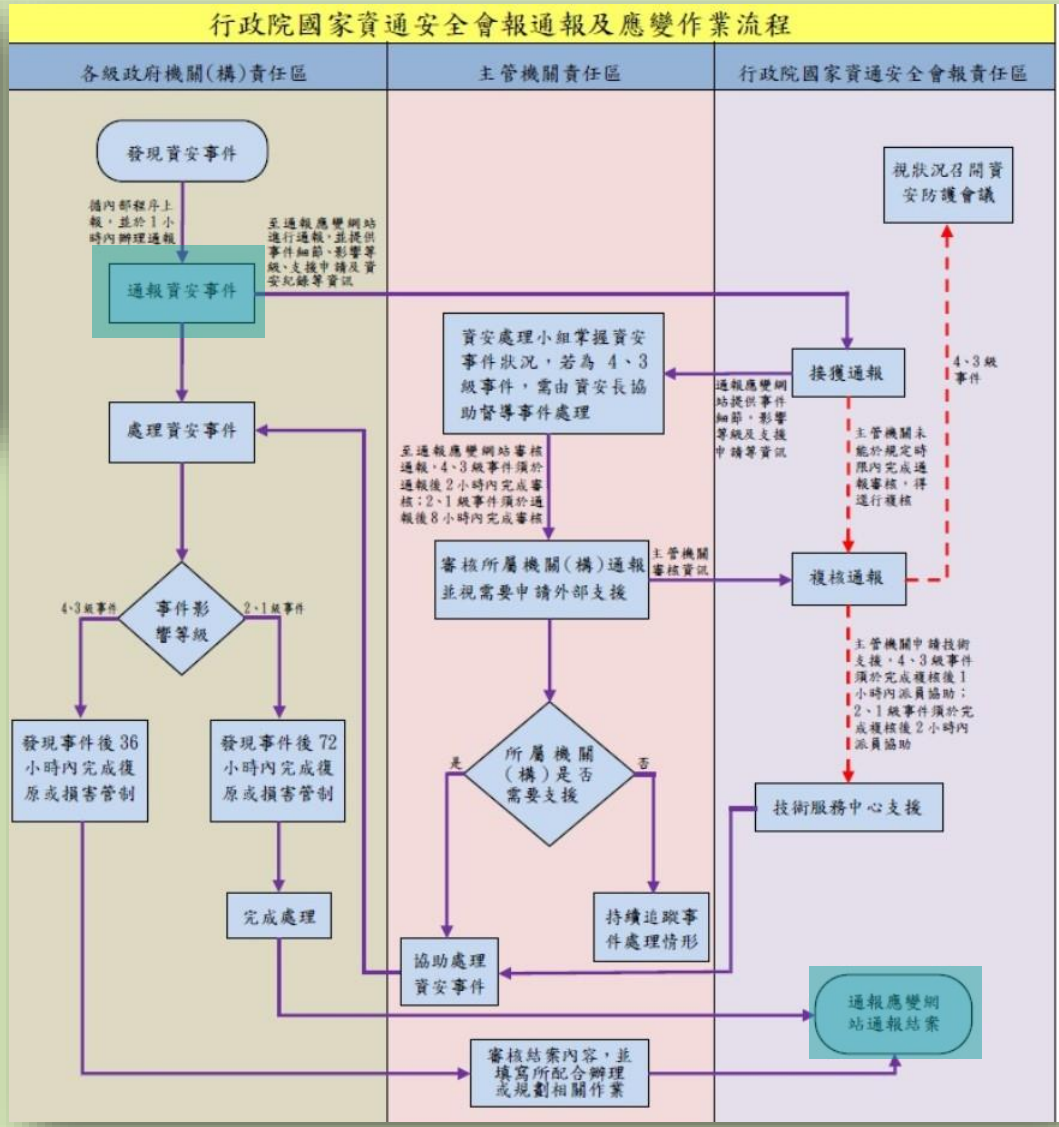
評估損失

# 通報追查


**7/2 上線**

- 通報應變網站提供政府機關事件通報管道
- 事件通報流程須完成通報登錄與結案

*https://www.ncert.nat.gov.tw/*



# 通報追查


(06)298-7777

708台南市安平區永華路二段208號

# Thank you for your attention!

Do you have any questions?