# 臺大區網網管會議

臺灣大學計算機及資訊網路中心

報告人：李美雯

大綱

OUTLINE

ASOC 資安偵測 & 情資分析

TANet DDoS 防護

漏洞與案例分析

01

# ASOC資安偵測 情資分析

# 情資偵測與分析

## 01 TALOS

使用Cisco TALOS 情資，包含：IP、domain、URL、挖礦、釣魚、惡意bot等黑名單，每天即時更新。

## 02 SNORT

使用商業版Snort rule，目前共有五萬餘條規則，並即時更新動態調整規則，常態開啟之規則約有1萬餘條。

## 03 ArcSight & ELK

使用 ArcSight 情資整合平台，撰寫事件關聯規則，以及自動化流程；使用ELK視覺化資料庫，進行事件分析，以及大數據應用。


## 七大區網中心

使用 Sourcefire IPS，包含：台大、政大、桃園、竹苗、新竹、宜蘭、南投，占全台年度開單事件量 59% 以上。

**100K**
Snort rules intrusion events
Per day

**17000K**
Security intelligence events

03

# TANet DDoS 防護

# TANet DDoS 防禦


60Gbps
最大可清洗 60Gbps 攻擊加正常流量。


OoP (Out of Path)

發現攻擊後，將流量導入清洗，平時不影響正常流量


- 外對內
- 內對外
- 內對內 (搭配南北聯防)

針對TANet內外部DDoS威脅予以抑制，同時，協防科技大樓國際線。


- A-SOC偵測通報
- 單位主動發現與通報
- 教育體系以外機關通報

遵循教育部「教育體系分散式阻斷服務防禦與應變作業規範」

# 臺灣大學 PTT 網段 DDoS 攻擊

2024/9/9 親俄駭客組織 NoName057 聲稱已對台灣公共目標發起 DDoS 攻擊活動

- NoName057 為親俄羅斯駭客組織
- NoName057 發起了一個 DDOSIA 專案
  提供志願者自動化攻擊工具參與攻擊行動，並提供前10名貢獻者獎金
- NoName057 提供志願者 MegaMedusa 工具
  (由親巴勒斯坦和親穆斯林的馬來西亞駭客組織 RipperSec 所開發)

04

# 漏洞與案例分享

# 電子郵件社交工程攻擊

# 偽冒教育部名義發送業務需求之郵件

【教育部113學年】大專校院師資人員通訊錄

回覆 全部回覆 轉寄 ...

tmdcu.ken@msa.hinet.net 代表教育部資訊公開平臺 <lee@udb.moe.edu.tw>
收件者

已停用此郵件的連結與其他功能，若要開啟該功能，請移動此郵件至 [收件匣]。
我們已將此郵件轉換為純文字格式。
Outlook 禁止存取下列可能不安全的附件：address.doc.

附檔為【教育部 113 學年 大專校院 人員通訊錄】，請惠存檢視！

<https://ssl.hinets.tw/matomo/matomo.php?idsite=1&rec=1&action_name=chiahui@g.ncu.edu.tw_doc_send10> ----------

---

教育部資訊公開平臺

# 偽冒資安院名義發送資安攻擊預警之郵件


[內容說明:]
轉發國家資通安全研究檢測防禦中心 資安訊息警訊

近期加密勒索軟體活動異常活躍。
加密勒索軟體使用 RSA-2048 與 AES-128 加密機制來加密檔案資料，所以遭到加密的檔案資料幾乎無法自行復原。國家資通安全科技中心根據被害者電腦的索軟體活樣本，製作了勒索軟體專殺工具。請注意查收附檔。

附件解壓密碼：123456

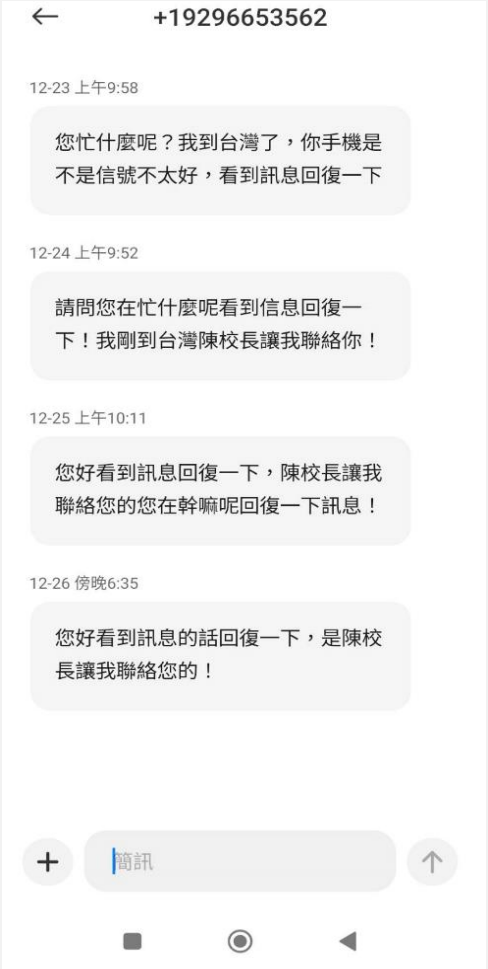
<https://ssl.hinets.tw/matomo/matomo.php?idsite=1&rec=1&action_name=hung@chai.tnua.edu.tw_2exe1209>
解壓后，雙擊“專殺軟體：trojan_killer”，出現如圖所示時，點擊【執行】。如未中勒索軟體，不會有任何提示；如若發現，則會提示殺毒軟體進行查殺。

如若出現藍色彈窗，請直接在壓縮文檔中運行，或嘗試點擊藍色彈窗的【更多】選項。

# 變臉恐嚇的勒索信件


[redacted]你好：
開門見山，我的目的很明確，只想求財，不想惹事。事情大概緣由簡單跟你闡述一下：我是私家偵探，受人之托對你進行了長期的跟蹤與調查，結果你也已經收到，在跟委托人溝通中發現，對方想法過于極端，想置你于死地，于是我私下給你發送這個郵件，收到郵件的你務必端正你的態度，第一時間聯系我協商處理，確保此視頻不再外流，花錢消災，我才能保證此事將不會對你的工作家庭帶來影響。過期未來電，一律視爲不處理態度，後果自負！
聯繫協商處理Line賬號：ws8888ws
扫快
在线
iQIYI
视频
讨论
梦回江湖
大话诛仙
16:22
02:27
选集

# 詐騙簡訊


+19296653562
12-23 上午9:58
您忙什麼呢？我到台灣了，你手機是不是信號不太好，看到訊息回復一下
12-24 上午9:52
請問您在忙什麼呢看到信息回復一下！我剛到台灣陳校長讓我聯絡你！
12-25 上午10:11
您好看到訊息回復一下，陳校長讓我聯絡您的您在幹嘛呢回復一下訊息！
12-26 傍晚6:35
您好看到訊息的話回復一下，是陳校長讓我聯絡您的！
簡訊

# 學術網域受到 SEO下毒

# 學術網域受到 SEO中毒

利用google Search的搜尋引擎最佳化**SEO**下毒，讓攻擊者的惡意網站於Google 上排名升高，導致使用者信任並訪問該惡意網站。

11月中旬，學術網路的部分網站受到SEO下毒，受攻擊的網站以老舊版本的XAMPP架站居多，後續再利用PHP CVE-2024-4577 漏洞入侵主機，也有些網站主機的管理者帳戶使用弱密碼，最終連線者被轉址到惡意網站。

# 防護作為建議

- 確認網站是否遭到入侵或被置入惡意程式。
  請特別確認該網站網頁內容是否有類似不當連結或有相關轉址的指令,以避免被不當轉址至其它惡意網頁。
  例如: HTML 網頁中的<header>區段被置入惡意轉址指令,導致使用 chrome 瀏覽器會被轉址到惡意網頁,但使用 Edge 開啟網頁則不會。

附錄一：Google Search Console 服務申請

1. 網站管理者至 Google Search Console 服務(網址：https://search.google.com/u/1/search-console/)申請管理帳號。


圖 1. Google Search Console 申請頁面

2. 請輸入網域資訊，接著即會繼續如圖 2 的驗證程序，請下載該認證檔，並上傳至網站(通常為網站根目錄(Documentroot))。




圖 2. Google Search Console 驗證程序

3. 在上傳完成後，即可完成驗證所有權，如圖 3 所示。


圖 3. 驗證成功訊息

# 防護作為建議

- 若已確認遭受SEO攻擊，建議網站管理者至 Google Search Console 服務申請管理帳號

- 申請完後可至Google Search Console服務申請「移除網址」以避免被他人查詢到錯誤的資訊。

附錄二：申請移除網址

1. 網站管理者登入 Google Search Console 服務後，先點選「(A)移除網址」，再點選「(B)新要求」後，即可輸入要清除的網址等資訊，待 Google 作業完成後，即可清除相關資訊。

3

# 防護作為建議

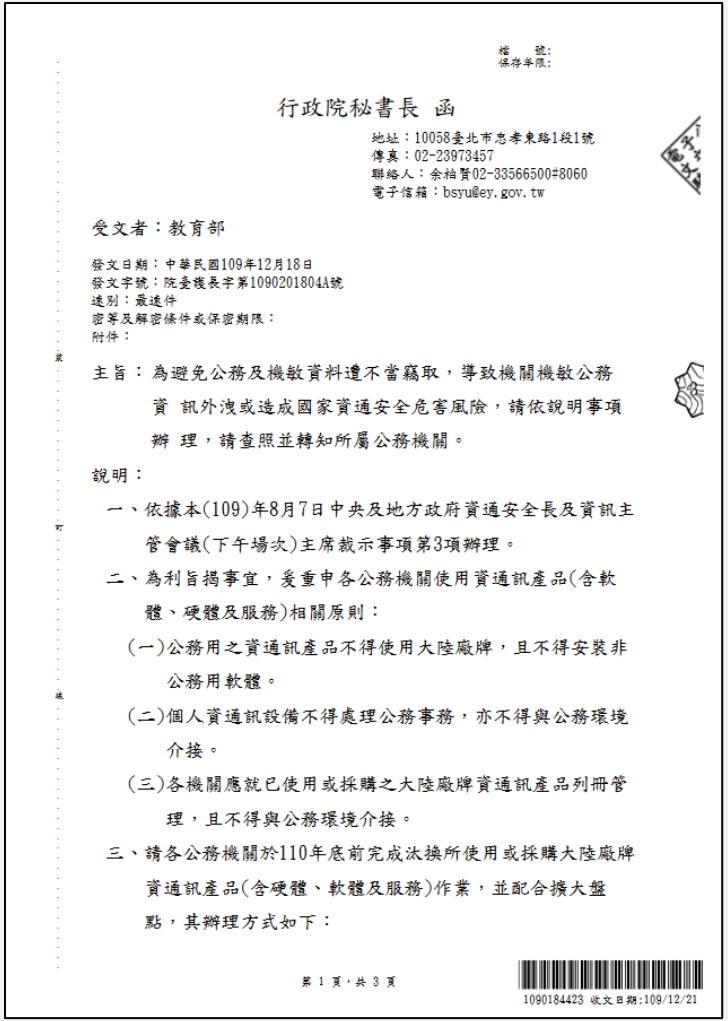
- 未來也可以定期透過 google 搜索學術網域，看是否有被 SEO 下毒，
  例如在 google 搜尋：site:edu.tw “股市”” 遊戲 “” 月餅 “….
- 建立robots.txt 檔案
- Google Search Console的權限，可定期確認網站是否有正常被Google引擎索引，
  檢索統計資料的報表亦可監控檢索狀況
- 因有時搜索結果會很多，北區ASOC有寫了一個小程式可以幫助匯出URL清單，
  後續可以方便資安人員驗證
- 若覺得有幫助可以在以下連結下載，雲端連結：
  https://drive.google.com/file/d/13RPYB_CtlnWIxa8RVGoIer_cHe2Ok0Qa/view?usp=sharing

# 陸製設備通報

TP-Link
海康威視

# 通報動機

- 鑑於物聯網設備應用蓬勃發展，**行政院**指示公務用之資通訊產品(含軟體、硬體及服務)**不得使用大陸廠牌**，以避免機關機敏公務資訊外洩或造成國家資通安全危害風險。
- **管理介面不可**暴露在**公開網路**上。



檔　號:
保存年限:

行政院秘書長 函

地址：10058臺北市忠孝東路1段1號
傳真：02-23973457
聯絡人：余柏賢02-33566500#8060
電子信箱：bsyu@ey.gov.tw

受文者：教育部

發文日期：中華民國109年12月18日
發文字號：院臺護長字第1090201804A號
速別：最速件
密等及解密條件或保密期限：
附件：

主旨：為避免公務及機敏資料遭不當竊取，導致機關機敏公務資訊外洩或造成國家資通安全危害風險，請依說明事項辦理，請查照並轉知所屬公務機關。

說明：

一、依據本(109)年8月7日中央及地方政府資通安全長及資訊主管會議(下午場次)主席裁示事項第3項辦理。

二、為利旨揭事宜，爰重申各公務機關使用資通訊產品(含軟體、硬體及服務)相關原則：

(一)公務用之資通訊產品不得使用大陸廠牌，且不得安裝非公務用軟體。

(二)個人資通訊設備不得處理公務事務，亦不得與公務環境介接。

(三)各機關應就已使用或採購之大陸廠牌資通訊產品列冊管理，且不得與公務環境介接。

三、請各公務機關於110年底前完成汰換所使用或採購大陸廠牌資通訊產品(含硬體、軟體及服務)作業，並配合擴大盤點，其辦理方式如下：

第 1 頁，共 3 頁

1090184423 收文日期:109/12/21

# 建議措施與結論

- 應立即停止與公務環境介接並汰換中國品牌設備。

- 拔除電源或設備斷網

- 請採購非中國設備，參考資料 :各機關對危害國家資通安全產品限制使用原則 http://www.rootlaw.com.tw/LawArticle.aspx?LawID=A040030001000900-1080418。

參考網址：https://www.blogger.com/blog/post/edit/9994984337261202 91/3164558707940028801?hl=zh-TW


Q & A