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。

Per day

100K
Snort rules intrusion events

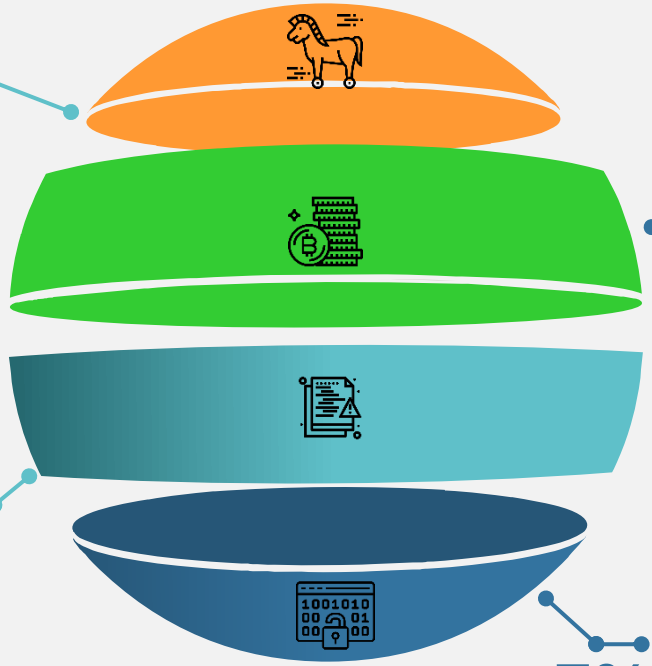
17000K
Security intelligence events

年度通報情資單種類

惡意中繼站

北區 ASOC 導入 IoC 外部情資，將主動對惡意中繼站連線 IP 進行通報，降低學網潛在風險。

32%



加密貨幣

加密貨幣與去年同期相比小漲，透過每週更新礦池阻擋與資安關懷，整體相較去年小幅下降7%。

19%

惡意程式

通報之惡意程式以WannaCry、Laplas、Zeus v3殭屍、Trojan與Redline佔據比例最高。

29%

漏洞通報

北區 ASOC 每月針對特定設備大型漏洞，或特定設備使用弱密碼暴露於 Internet，進行開單通報

7%

出處:北區ASOC團隊-統計數據:112年2月至112年9月

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」

04

漏洞與案例分享

XOOPS站長工具箱模組漏洞

NASOC-Rule SERVER-OTHER Adminer privilege escalation attempt

通報動機

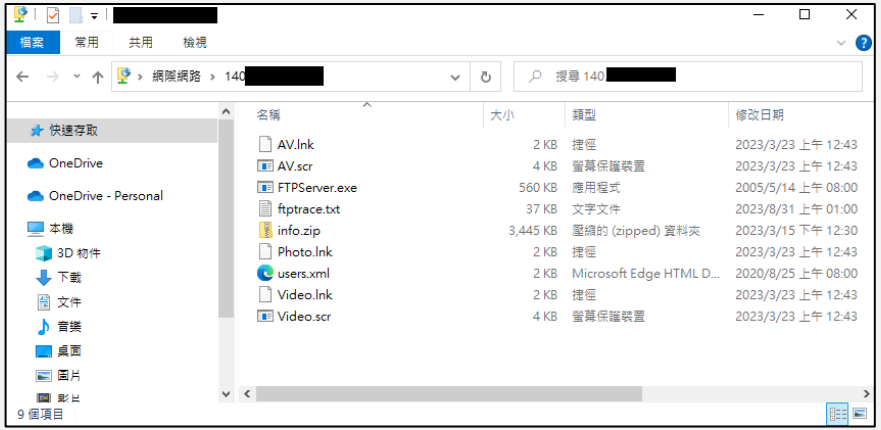
- XOOPS CMS網站內容管理系統近期發現嚴重資安漏洞已被利用植入惡意程式。
- 管理人員後台介面-站長工具箱模組中的**pma.php**有多個已知且CVSS高達9.8分的漏洞(滿分10分)，該頁面若使用預設密碼或遭暴力密碼破解成功，攻擊者將得到系統完整控制權。
- 北區ASOC已協助於112/08/02(三)。

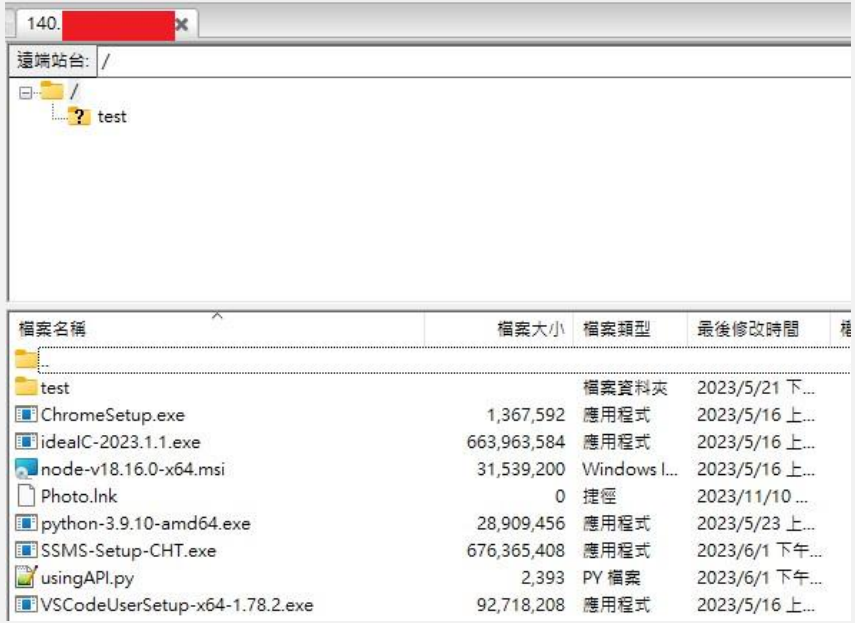
Adminer漏洞參考網址：https://www.cvedetails.com/vulnerability-list/vendor_id-17755/Adminer.html

設備預設帳號密碼登入通報

登入檢測(PhotoMiner蠕蟲病毒)

- 隨機對暴露在公開網路上使用**FTP協定的IP**，以內建的帳號密碼字典檔進行**暴力破解攻擊**，若使用弱密碼或匿名登入容易被此類型的蠕蟲病毒入侵。





參考網址：https://portal.cert.tanet.edu.tw/docs/pdf/20170929010955558577122890605 1.pdf

建議措施與結論

- 建議將設備放置於內部網路，若有外部網路存取需求，請限定連線IP(ACL)。
- 關閉預設帳號與匿名登入服務，並使用強度較高的密碼。
- 若有放置機敏性資料的需求，請進行加密或作適當的遮罩，並於使用完畢後移除以降低風險。
- 依據檔案的重要性與機密性建立權限控管機制。
- 定期檢視系統稽核紀錄降低資安風險。

Thank You !

Q & A