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

案例分析與物聯網通報

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

2025年第二季區網 Top 3 情資

區網中心	事件
臺大區網	1.**Zeus V3惡意程式** (共 38 筆，佔總量 17.35%) MALWARE-CNC Win.Trojan.Zeus v3 DGA DNS query detected
	2.**Relevantknowledge 間諜軟體**(共 22 筆，佔總量 10.05%) MALWARE-OTHER Trackware relevantknowledge runtime detection
	3.**OpenSSH競爭條件漏洞**(共 15 筆，佔總量 6.85%) NASOC-Rule OpenSSH Vulnerability Risk (CVE-2024-6387)

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

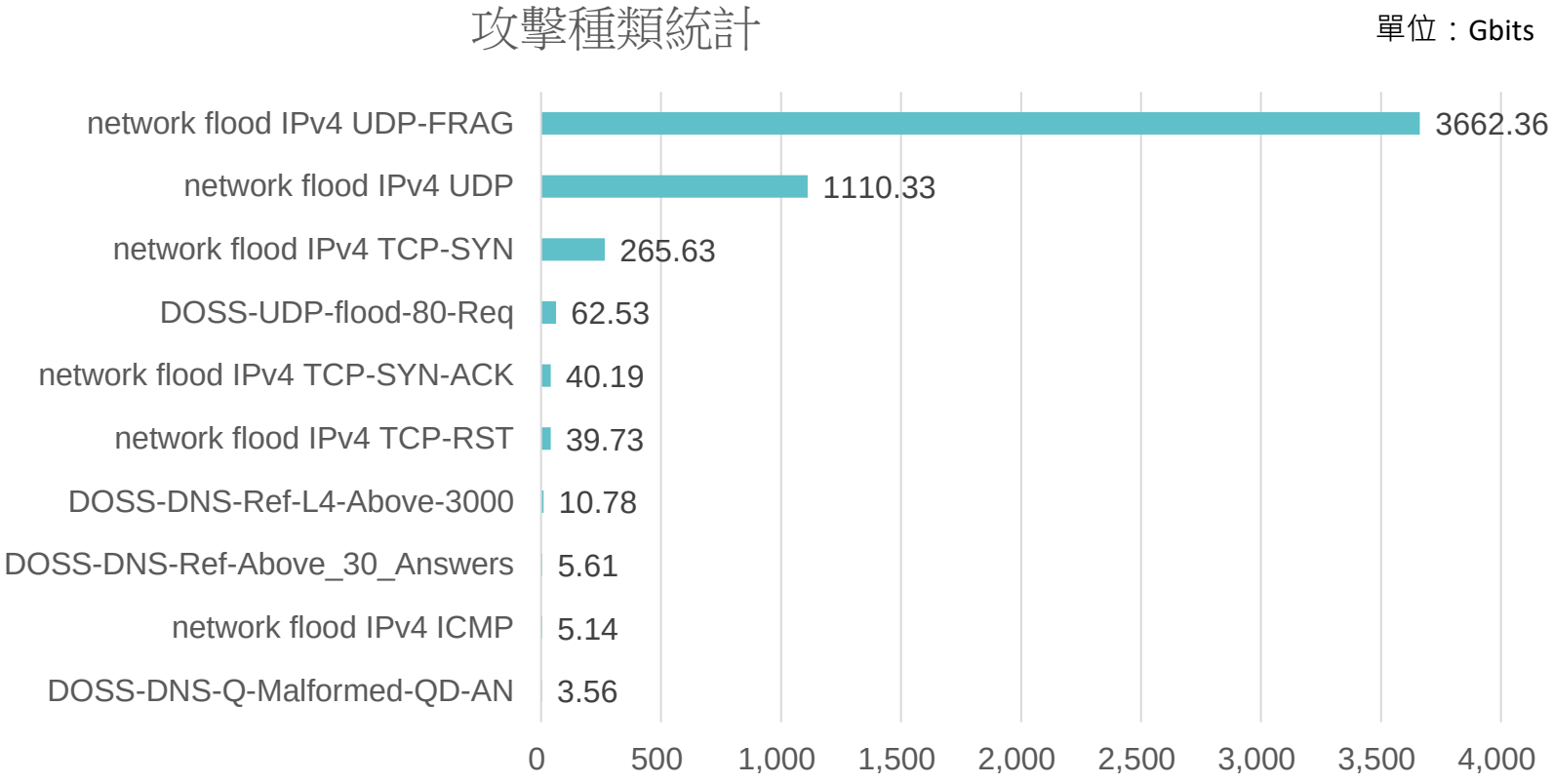
- 外對內
- 內對外
- 內對內 (搭配南北聯防)

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」

2025年第二季DDoS攻擊總流量與攻擊類型排行



攻擊清洗總流量約 5.2 Tbits

備註：2025年第二季DDoS攻擊統計日期為2025/03~2025/05

04

案例分享與物聯網通報

殭屍網路AyySSHush利用

CVE-2023-39780

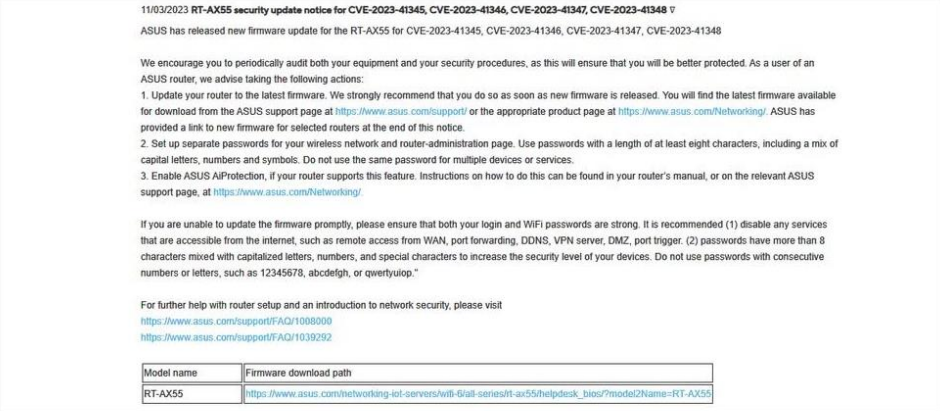
前言

新聞

針對遭殭屍網路AyySSHush利用的路由器漏洞，華碩針對這些資安弱點公告提出說明

殭屍網路AyySSHush鎖定華碩路由器CVE-2023-39780等3項漏洞而來，入侵並控制約9千臺路由器，而對於這些漏洞修補的情況，我們也進一步詢問華碩，他們表示先後於2023年及今年4月修補

文/ 周峻佑 | 2025-06-03 發表



11/03/2023 **RT-AX55 security update notice for CVE-2023-41345, CVE-2023-41346, CVE-2023-41347, CVE-2023-41348**

ASUS has released new firmware update for the RT-AX55 for CVE-2023-41345, CVE-2023-41346, CVE-2023-41347, CVE-2023-41348

We encourage you to periodically audit both your equipment and your security procedures, as this will ensure that you will be better protected. As a user of an ASUS router, we advise taking the following actions:

1. Update your router to the latest firmware. We strongly recommend that you do so as soon as new firmware is released. You will find the latest firmware available for download from the ASUS support page at https://www.asus.com/support/ or the appropriate product page at https://www.asus.com/Networking/. ASUS has provided a link to new firmware for selected routers at the end of this notice.
2. Set up separate passwords for your wireless network and router-administration page. Use passwords with a length of at least eight characters, including a mix of capital letters, numbers and symbols. Do not use the same password for multiple devices or services.
3. Enable ASUS AiProtection, if your router supports this feature. Instructions on how to do this can be found in your router's manual, or on the relevant ASUS support page, at https://www.asus.com/Networking/.

If you are unable to update the firmware promptly, please ensure that both your login and WiFi passwords are strong. It is recommended (1) disable any services that are accessible from the internet, such as remote access from WAN, port forwarding, DDNS, VPN server, DMZ, port trigger. (2) passwords have more than 8 characters mixed with capitalized letters, numbers, and special characters to increase the security level of your devices. Do not use passwords with consecutive numbers or letters, such as 12345678, abcdefgh, or qwertyuiop."

For further help with router setup and an introduction to network security, please visit
https://www.asus.com/support/FAQ/1008000
https://www.asus.com/support/FAQ/1039292

Model name	Firmware download path
RT-AX55	https://www.asus.com/networking-iot-servers/wifi-6/all-series/rt-ax55/helpdesk_bios/?model2Name=RT-AX55

上週威脅情報業者GrayNoise揭露鎖定華碩路由器而來的殭屍網路AyySSHush攻擊行動，並指出過程當中駭客運用已知漏洞CVE-2023-39780與兩個未登記CVE編號的弱點，停用與趨勢科技合作的內建防護機制AiProtection，從而控制約9千臺

參考資料：
https://www.ithome.com.tw/news/169322

事件說明

威脅情報業者GrayNoise揭露鎖定華碩路由器而來的殭屍網路AyySSHush攻擊行動

- 新聞發布確定受到影響的型號為:RT-AX55、RT-AC3100、RT-AC3200
- 使用 port:53282 為 ssh 連線，持久控制設備
- 學網相關設備並無開啟 port:53282，暫時沒有受到影響

偵測53282 port 疑似受影響型號
ZENWIFI
LYRA
RT-AC88U
RT-AX55
TUF-AX3000
RT-AC5300
RT-AX82U
GT-AC5300
RT-AC3100
BLUE CAVE

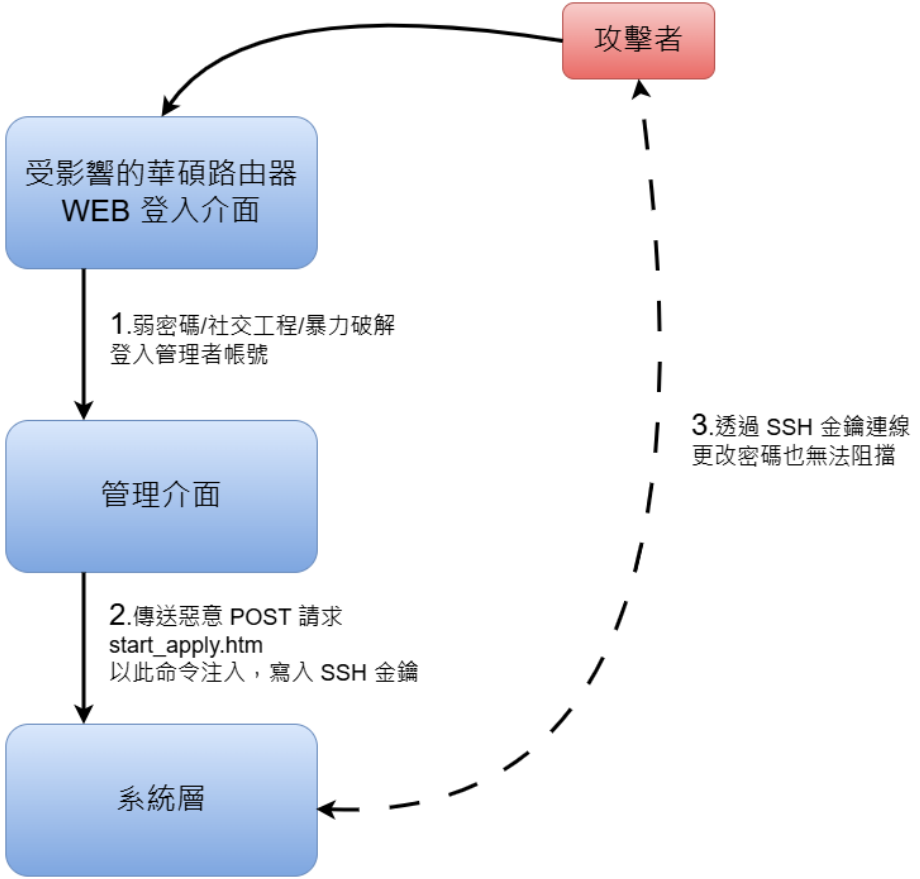
參考資料：
https://censys.com/blog/tracking-ayysshush-a-newly-discovered-asus-router-botnet-campaign
https://www.asus.com/networking-iot-servers/wifi-routers/all-series/rt-ax55/

漏洞描述

1. 弱密碼/社交工程/暴力破解
   登入管理者帳號

2. 傳送惡意 POST 請求至
   start_apply.htm
   後續寫入 ssh 金鑰

3. 攻擊者可透過金鑰連線，
   更改密碼無法阻擋



建議處理措施

- 相關設備已經 EOL
- 華碩聲稱更新至最新版本即可防止此漏洞攻擊
- 建議使用強密碼
- 禁用 ssh 遠端功能，檢查是否關閉 port : 53282

➢ ASOC 已有針對學網暴露在外的路由器發信通知 (華碩IP分享器公開登入介面有 91 台)

華碩關於最近有關路由器安全性的報告的官方聲明

2025/06/04

加利福尼亞州弗里蒙特，2025 年 6 月 4 日 - 針對最近媒體關於試圖利用華碩路由器漏洞的報導，華碩希望傳達這些漏洞可以修復的資訊。雖然有些人指出僅靠固件更新可能無法完全解決問題，但華碩想強調以下建議 — 包括更新到最新固件、執行出廠重置和設置強管理員密碼 — 以有效恢復和維護設備安全。

下面概述的步驟不僅對於降低潛在風險至關重要，而且對於在當今不斷變化的網路安全環境中加強長期保護和負責任的設備管理也至關重要。

固件更新和強密碼可以有效防止未來風險

這些媒體報導涉及 2023 年披露的安全漏洞（CVE-2023-39780）。已使用最新固件更新並使用強管理員密碼保護的設備可以防止將來利用此漏洞並阻止類似的攻擊方法。

建議使用者使用至少 10 個字元長的密碼，並包含大寫和小寫字母、數位和符號。此外，ASUS 建議使設備固件保持最新狀態，以確保持續保護。

可能受影響的設備可以完全恢復

如果設備之前使用過時的韌體和弱密碼，並且使用者懷疑它可能已被洩露，請按照以下步驟保護設備：
1. 將韌體更新到最新版本
2.執行恢復出廠設置以清除任何未經授權或異常的設置
3.如上所述
設置強管理員密碼
這些步驟將確保設備完全安全，並且不會留下任何殘留風險。

壽命終止（EOL）設備仍然可以安全使用

對於不再接收固件更新的 EOL 設備，建議採用以下最佳實踐：
1. 為設備
安裝最新的可用韌體版本 2.使用強管理員密碼
3.禁用所有遠端訪問功能，例如 SSH、DDNS、AiCloud 或 WAN 的

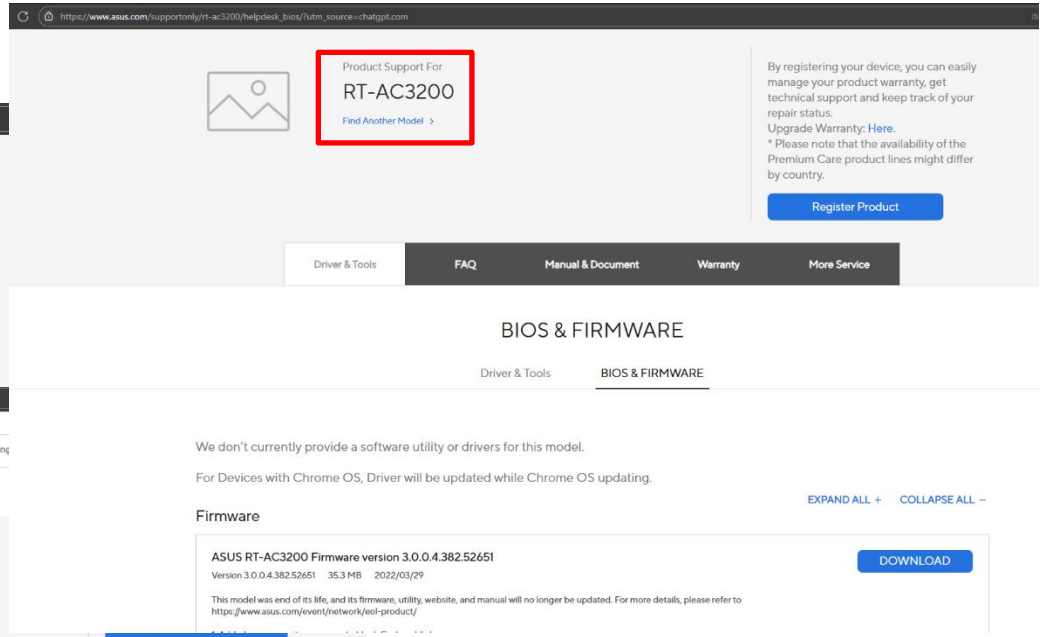
Web 訪問完成上述步驟將有效防止最近報告中描述的漏洞利用方法。

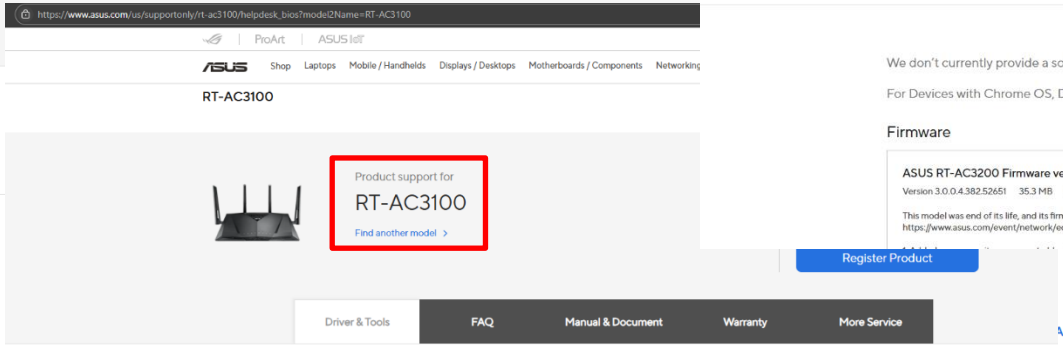
針對可疑活動的可選自檢

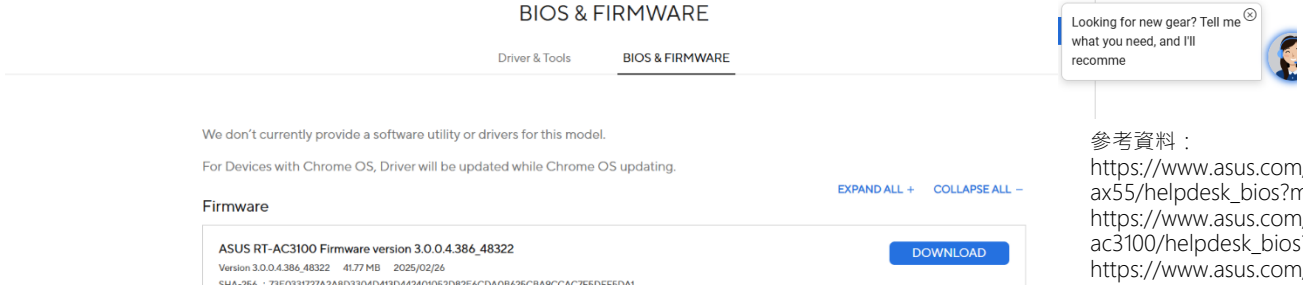
使用者可以執行以下檢查以確定他們的設備是否顯示出未經授權訪問的跡象：
1. 確認 SSH（尤其是 TCP 連接埠 53282）沒有暴露在互聯網
上 2.檢查系統紀錄中是否有重複登入失敗或不熟悉的 SSH 金鑰

參考資料：
https://www.asus.com/us/news/wbhfio4vqjodds5p/

建議處理措施







參考資料：
https://www.asus.com/networking-iot-servers/wifi-routers/all-series/rt-ax55/helpdesk_bios?model2Name=RT-AX55
https://www.asus.com/us/supportonly/rt-ac3100/helpdesk_bios?model2Name=RT-AC3100
https://www.asus.com/supportonly/rt-ac3200/helpdesk_bios/

台灣某大學遭到Nova勒索軟體攻擊

前言

資安拉警報！逢甲大學證實遭勒索病毒NOVA攻擊：已急防擴散

綜合中心

2025年6月20日 週五 上午9:15

逢甲大學校門口，取自逢甲大學臉書

媒體報導勒索病毒NOVA攻擊亞洲兩所大學，包括南韓顯文大學和我國的逢甲大學。對此，逢甲大學昨（6/19）晚發出聲明證實，17日即接獲外部情資，得知被勒索病毒NOVA集團鎖定，已初步確認受害範圍與原因，並採取必要措施避免擴散。

有媒體報導指出，NOVA這次入侵拿到10GB資料，包含一些程式碼、員工數據、學生付款紀錄、數據庫架構，如果逢甲大學不回應NOVA的要求，10天後部分資料將會對外公開。報導並指，NOVA罕見在暗網上標註，攻打逢甲大學的是「Chinese APT | Nova Affiliates」，恐是具有國家級背景的駭客組織，引起資安界關注。

參考資料：
Yahoo新聞

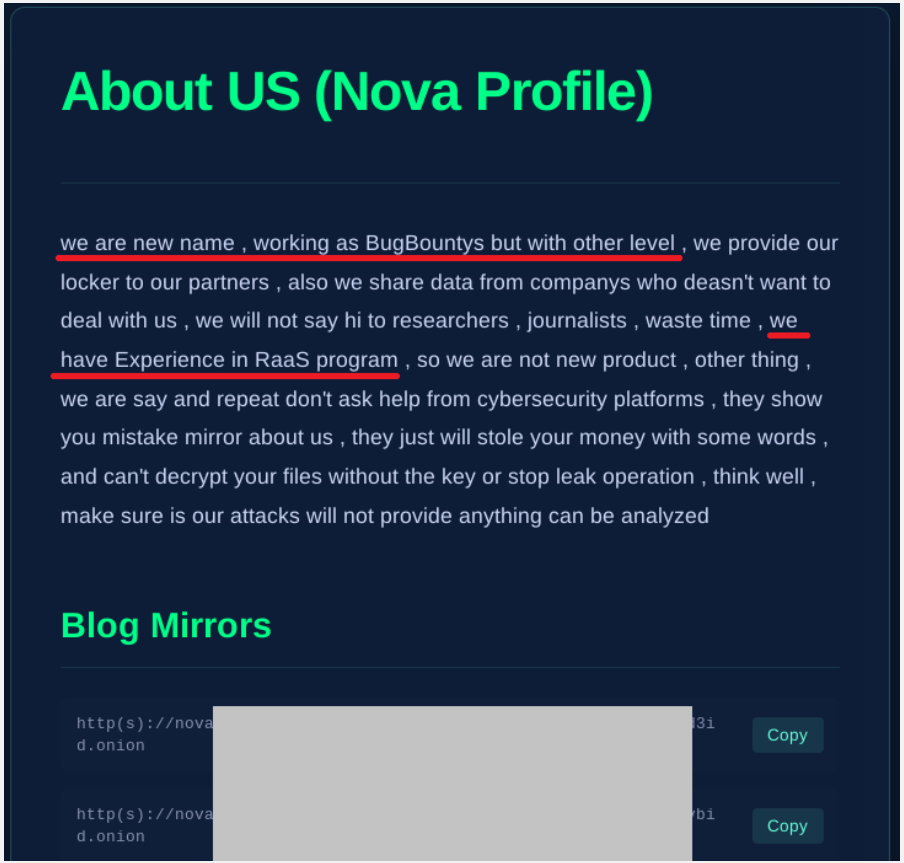
Nova是誰?

- 根據各資安公司的公布消息，前身名為RALord，約在2025年3月下旬出現。
- 已經有經營RaaS (Ransomware-as-a-Service)項目。
- 2025年4月30日， RALord 更名為 Nova，詳細原因不明。

參考資料：
俊盟科技
https://blog.billows.com.tw/?p=3766&fbclid=IwQ0xDSwLASQpleHRuA2FlbQIxMQABHisfRAccyv48fTqJDf1y5__jU_kskAGFPtRModYqyL32D6fAq0KbmHKX5BXY_aem_Au2X2YhCuni7V4pj3TI3HQ
CYJAX
https://www.cyjax.com/resources/blog/araastocracy-ralord-ransomware-emerges-with-new-dls/

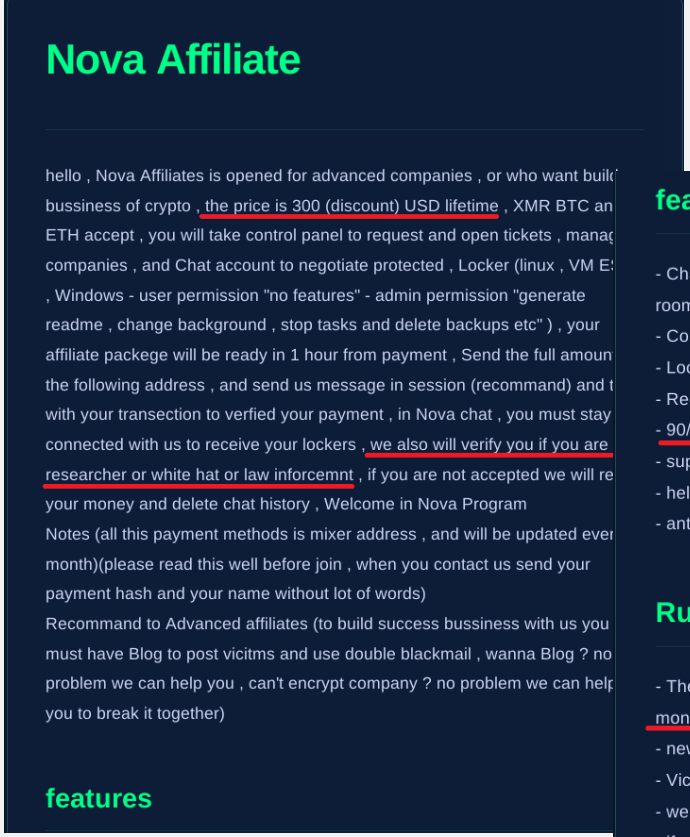
Nova是誰?

- Nova 聲稱他們比一般的漏洞賞金獵人技術更高名。
- 擁有RaaS的經驗 (代表Nova已有多年經驗，非新成立的駭客團體)。
- 根據 CYJAX 的說明，RALord 的原始部落格包含英語和俄語內容，這很可能代表該組織來自使用俄語的國家。



Nova提供的服務

- 開放加盟Nova，目前優惠300美金(終身)。
- Nova會驗證身分，拒絕資安研究員、白帽駭客、執法人員。
- 90/10 for affiliate
  收到贖金後，加盟者可獲得90%利潤，Nova獲得10%利潤。
- 一個月內未攻擊成功的加盟者，會被Nova封鎖。



Nova Affiliate

hello , Nova Affiliates is opened for advanced companies , or who want built bussiness of crypto , the price is 300 (discount) USD lifetime , XMR BTC an ETH accept , you will take control panel to request and open tickets , manag companies , and Chat account to negotiate protected , Locker (linux , VM E , Windows - user permission "no features" - admin permission "generate readme , change background , stop tasks and delete backups etc") , your affiliate packege will be ready in 1 hour from payment , Send the full amoun the following address , and send us message in session (recommand) and t with your transection to verfied your payment , in Nova chat , you must stay connected with us to receive your lockers , we also will verify you if you are researcher or white hat or law inforcemnt , if you are not accepted we will re your money and delete chat history , Welcome in Nova Program

Notes (all this payment methods is mixer address , and will be updated ever month)(please read this well before join , when you contact us send your payment hash and your name without lot of words)

Recommand to Advanced affiliates (to build success bussiness with us you must have Blog to post vicitms and use double blackmail , wanna Blog ? no problem we can help you , can't encrypt company ? no problem we can help you to break it together)

features

- Chat system for affiliates , create advanced and costumize negotiation chat rooms , request lockers
- Control panel to organize attacks and request lockers
- Lockers (Linux , windows , Vmware ESXI) (request)
- Request to post in our BLOG
- 90/10 for affiliate
- support 24/7
- help for attacks and guide
- anti detection and anti analyst for all lockers (0 capture)

Rules

- The affiliates who doesn't been in touch or Doesn't made success attacks in 1 month will be Banned
- new affiliates need to be focused to learn and start they business
- Victims will be posted on our BLOG
- we provide just Lockers and guide (No RATs , Payloads , or other malwares)
- if you know your self can't make success attacks or work serious don't contact or join

Mixers Payment Methods - ~~$800~~ $300

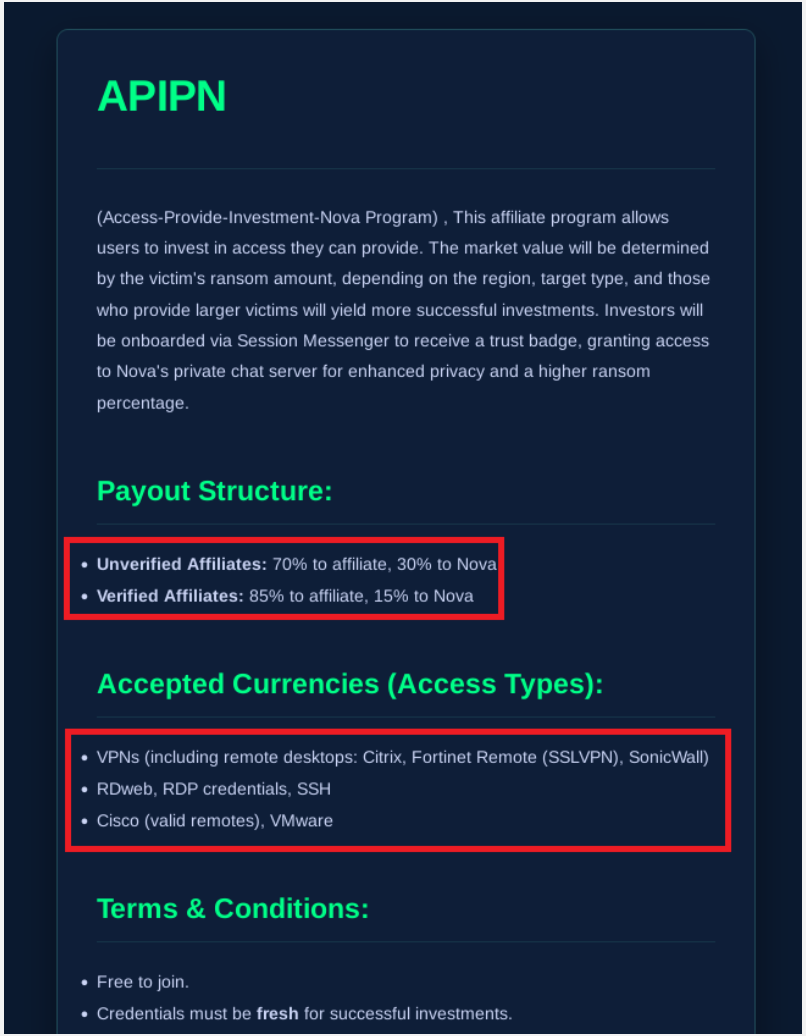
1D1T7 BTC

Nova提供的服務

- 投資Nova計劃(免費加入)，加入者可提供已洩漏的憑證，Nova後續會進行攻擊。

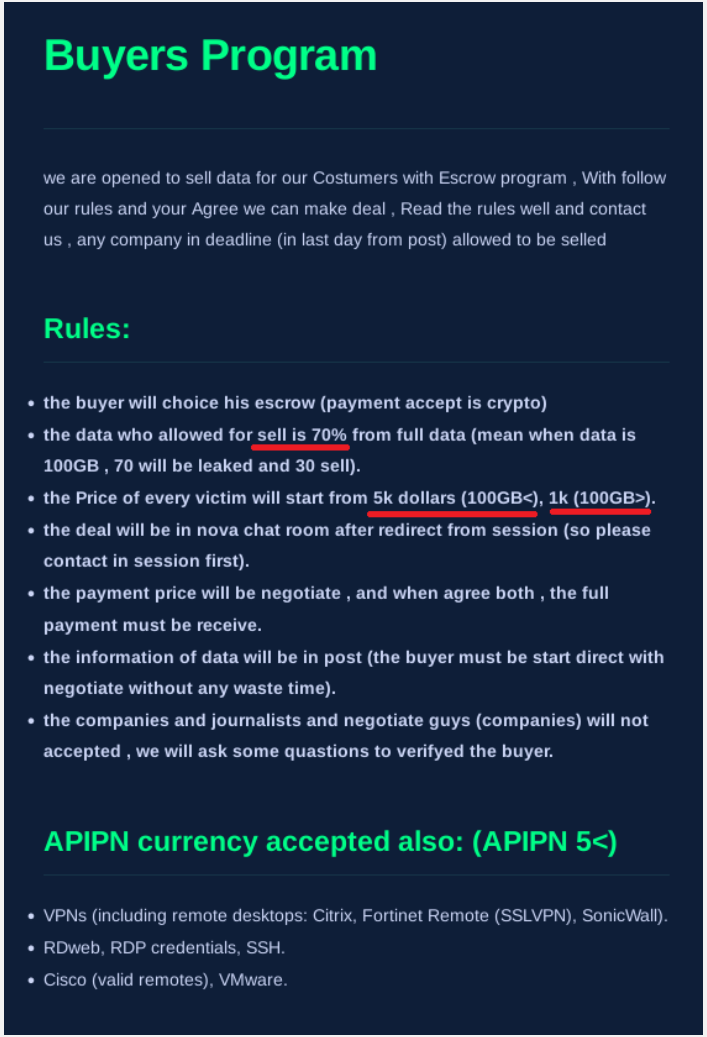
- 收到贖金後，
  未驗證的會員獲得70%利潤，Nova獲得30%利潤。
  已驗證的會員獲得85%利潤，Nova獲得15%利潤
  (已驗證的條件需提供15個以上憑證，及可以順利登入)。

- 接受憑證類型
  VPNs (including remote desktops: Citrix, Fortinet Remote (SSLVPN), SonicWall)
  RDweb, RDP credentials, SSH
  Cisco (valid remotes), VMware



Nova提供的服務

- 開放資料出售，出售全部資料的70%。
- 每個受害者小於100GB資料，價格為5000美金，大於100GB資料，價格為1000美金 (應是資料量越大，實際有用的資訊比例越低的因素)。
- 開放已洩漏憑證當作交換籌碼，
  VPNs (including remote desktops: Citrix, Fortinet Remote (SSLVPN), SonicWall)
  RDweb, RDP credentials, SSH
  Cisco (valid remotes), VMware



Buyers Program

we are opened to sell data for our Costumers with Escrow program , With follow our rules and your Agree we can make deal , Read the rules well and contact us , any company in deadline (in last day from post) allowed to be selled

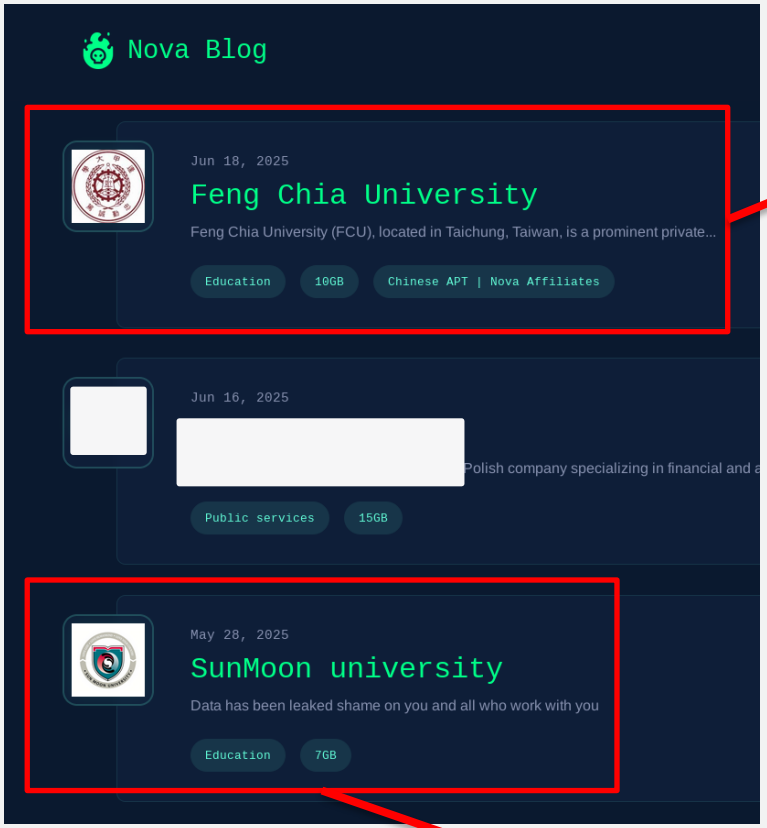
Rules:

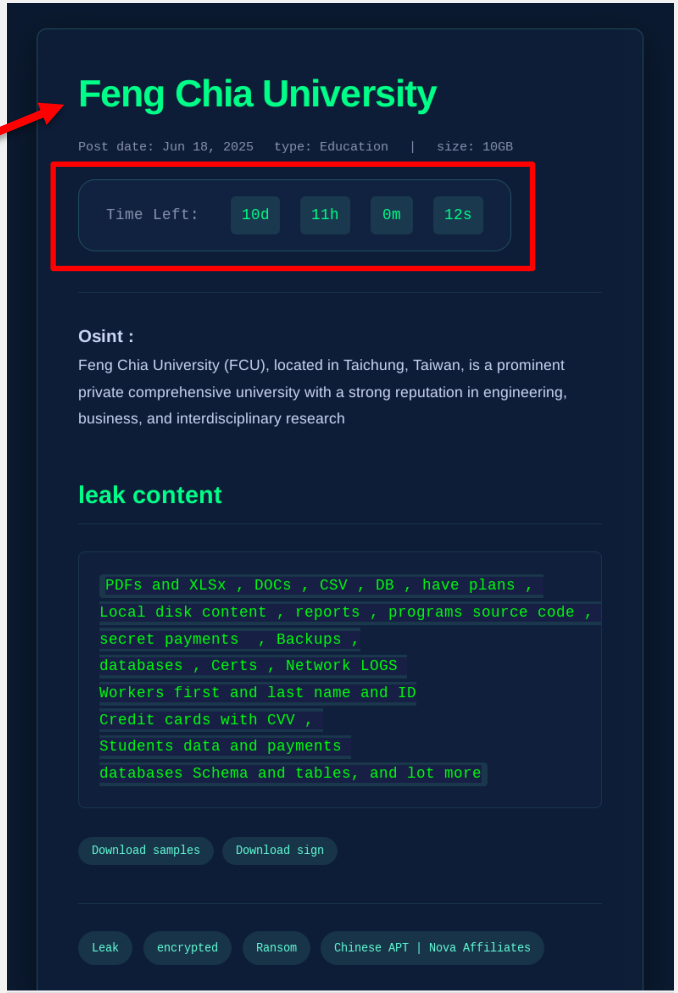
- the buyer will choice his escrow (payment accept is crypto)
- the data who allowed for sell is 70% from full data (mean when data is 100GB , 70 will be leaked and 30 sell).
- the Price of every victim will start from 5k dollars (100GB<), 1k (100GB>).
- the deal will be in nova chat room after redirect from session (so please contact in session first).
- the payment price will be negotiate , and when agree both , the full payment must be receive.
- the information of data will be in post (the buyer must be start direct with negotiate without any waste time).
- the companies and journalists and negotiate guys (companies) will not accepted , we will ask some quastions to verifyed the buyer.

APIPN currency accepted also: (APIPN 5<)

- VPNs (including remote desktops: Citrix, Fortinet Remote (SSLVPN), SonicWall).
- RDweb, RDP credentials, SSH.
- Cisco (valid remotes), VMware.

Nova勒索公告平台

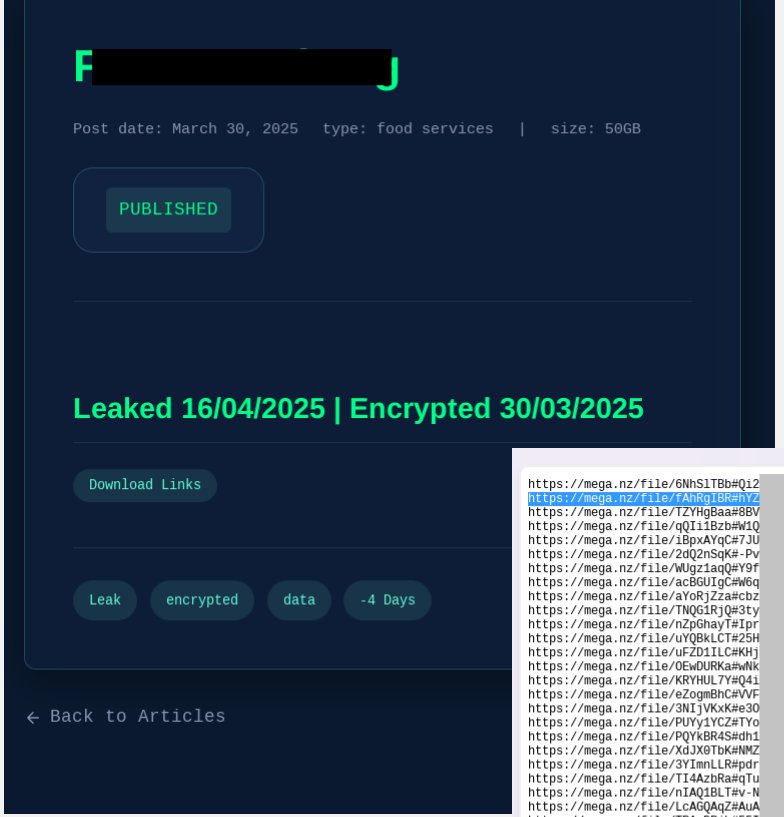


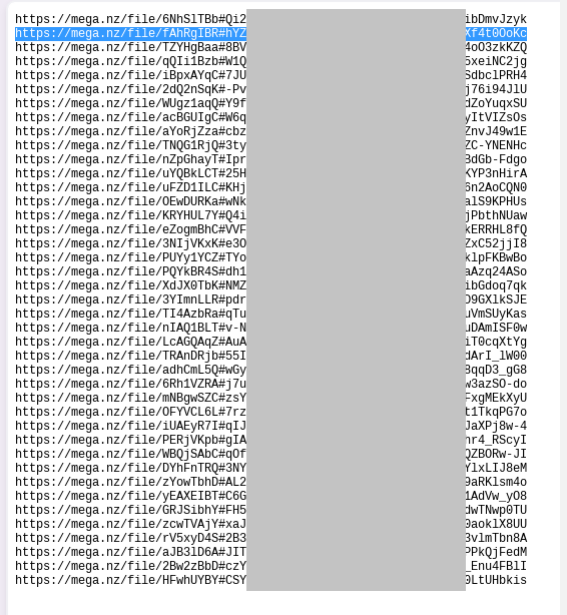


- 南韓顯文大學資料已被公開

Nova勒索公告平台

- 台灣某知名滷肉飯業者的資料已被公開。
- 檔案下載連結已被公布。





預防措施

- 定期備份，可參考3-2-1備份原則，
  3- 至少要保留三份資料副本，原始資料和兩份備份。
  2- 備份資料應儲存在至少兩種不同的儲存媒體上，例如硬碟、外接硬碟、雲端。
  1- 至少一份備份應儲存在與原始資料不同的物理位置。

- 實施最小權限原則，避免一般使用者擁有管理權限。

- 實施多因素驗證(MFA)。

- 定期修補漏洞，尤其是暴露在公開網路的服務或遠端連線系統。

- 部屬EDR偵測。

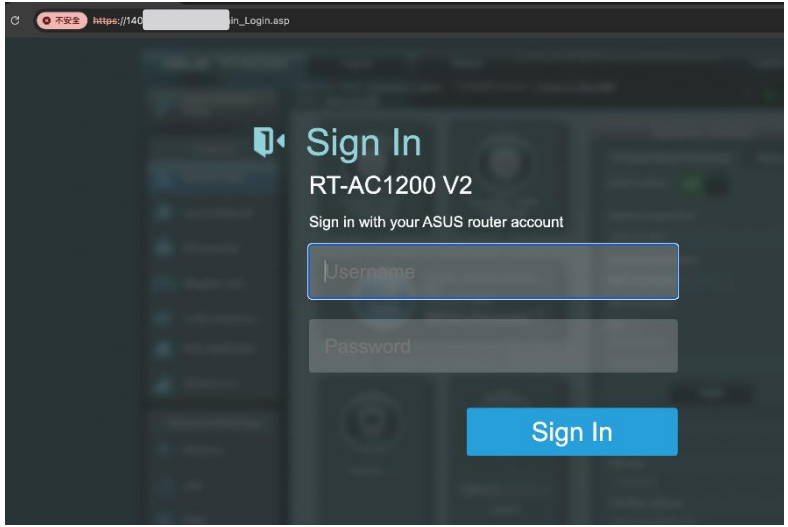
- 建立分段的網路架構，避免橫向擴散導致整個組織被入侵。

IoT偵測報告

1. IP分享器管理介面
2. 印表機管理介面
3. ftp匿名登入
4. 大陸廠牌資通訊產品

IP分享器管理介面

- 利用 shodan 找尋學網有關網路設備的IP，查詢設備類型或廠牌名稱等。
- 查詢到後再透過實際連線測試，查看是否可被外部IP連線到登入介面。



隱藏風險:

1.攻擊者可嘗試弱密碼登入或暴力破解。
2.查詢此型號已知漏洞，嘗試漏洞利用(Exploit)。
3.若攻擊者入侵成功，可能修改 DNS 設定、橫向移動或建立後門等等。

建議處理措施(擇一):

1.設定 ACL，只讓管理者 IP 可以連線。
2.移到內部網路，可搭配使用 VPN、ACL、跳板機等機制管控。

印表機管理介面

- 利用 shodan 找尋學網有關網路設備的IP，查詢設備類型或廠牌名稱等。
- 查詢到後再透過實際連線測試，查看是否可被外部IP連線到登入介面。

◘ 隱藏風險:

1.如有登入介面，攻擊者可嘗試弱密碼登入、暴力破解，或根據印表機型號嘗試漏洞利用(Exploit)。
2.直接顯示管理介面可能洩漏列印記錄、使用者帳號、系統資訊等等。
3.可能受到未授權操作，重設印表機設定或Email外傳列印資料等等。

◘ 建議處理措施(擇一):

1.設定 ACL，只讓管理者 IP 可以連線。
2.移到內部網路，可搭配使用 VPN、ACL、跳板機等機制管控。

Shodan搜尋 – 印表機

印表機常見廠牌名稱
brother
canon
dell
epson
Fuji
xerox
hp
konica
kyocera
lexmark
oki
ricoh
samsung
sharp
toshiba

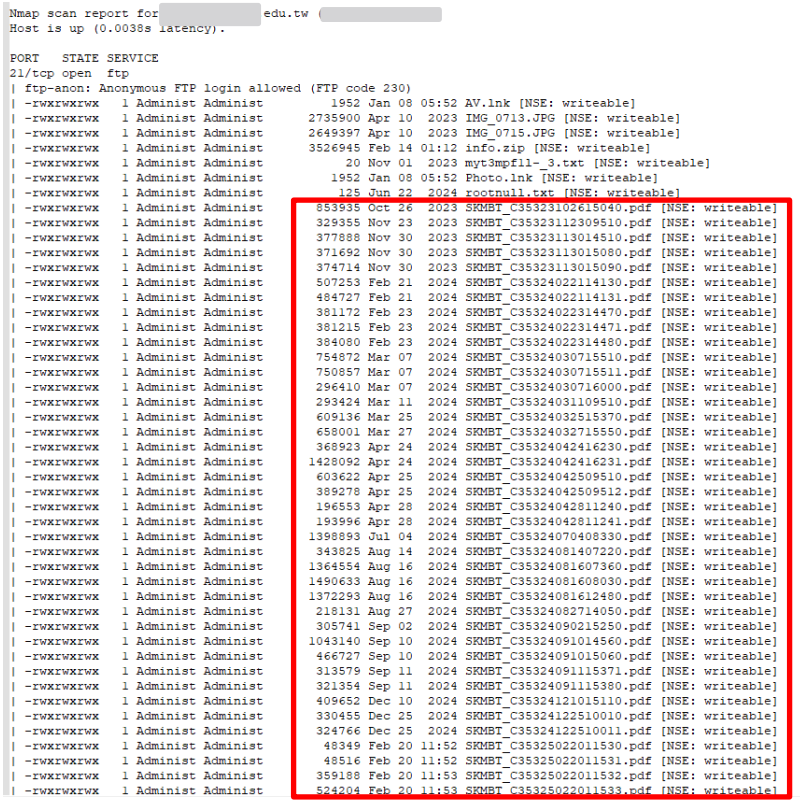
port號可更換做掃描

或刪除 port 號，
直接查詢網段印表機

語法參考
brother port:9100 net:192.168.0.0/16
canon port:9100 net:192.168.0.0/16
dell port:9100 net:192.168.0.0/16
epson port:9100 net:192.168.0.0/16
Fuji port:9100 net:192.168.0.0/16
xerox port:9100 net:192.168.0.0/16
hp port:9100 net:192.168.0.0/16
konica port:9100 net:192.168.0.0/16
kyocera port:9100 net:192.168.0.0/16
lexmark port:9100 net:192.168.0.0/16
oki port:9100 net:192.168.0.0/16
ricoh port:9100 net:192.168.0.0/16
samsung port:9100 net:192.168.0.0/16
sharp port:9100 net:192.168.0.0/16
toshiba port:9100 net:192.168.0.0/16

ftp 匿名登入

- 利用 shodan 找尋有開啟 port:21 的設備。
- 測試是否可以匿名登入。



隱藏風險:

1.未授權的檔案下載(個資外洩)。
2.可能遭到未授權檔案上傳(惡意程式)。

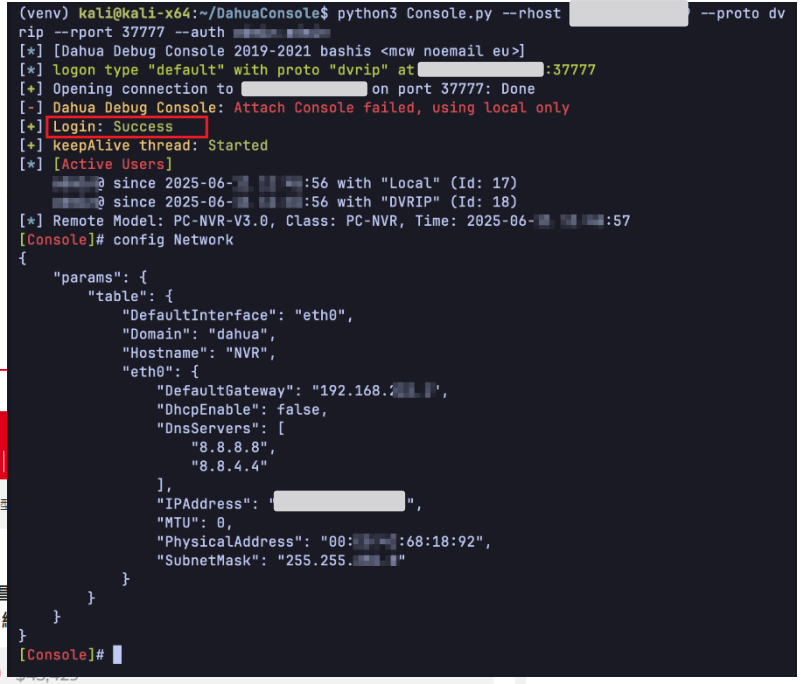
建議處理措施:

1.關閉匿名登入功能。
2.非必要服務應移置內網。
3.必要服務應設定好權限，及關閉上傳功能。

大陸廠牌資通訊產品

- 利用 shodan 找尋大陸廠牌攝影機
  - EX：net: 192.168.1.0/24 Dahua

- Web登入介面
  NVR主機
  貼牌產品



參考資料:
https://github.com/mcw0/DahuaConsole

Shodan搜尋 –大陸廠牌資通訊IoT產品 (常見/疑似)

被視為大陸廠牌資通訊產品	常見的IOT類型	語法參考
DJI (大疆)	無人機、穩定器、攝影機	DJI net:192.168.0.0/16
Foscam	網路攝影機、智慧家庭監控	Foscam net:192.168.0.0/16
Hisense (海信)	智慧電視、智慧冰箱、智慧空調	Hisense net:192.168.0.0/16
Huawei (華為)	路由器、智慧音箱、智慧穿戴、智慧家庭hub	Huawei net:192.168.0.0/16
Hytera (海能達)	對講機、無線通訊設備	Hytera net:192.168.0.0/16
Insta360 (影石創新)	全景攝影機、運動攝影機	Insta360 net:192.168.0.0/16
Lenovo (聯想集團)	智慧顯示器、智慧家庭hub、平板電腦	Lenovo net:192.168.0.0/16
Meizu (魅族)	智慧手機、智慧家庭設備	Meizu net:192.168.0.0/16
MI (小米)	智慧手機、智慧音箱、掃地機器人、智慧燈泡、監控攝影機	xiaomi net:192.168.0.0/16
Nubia (努比亞)	智慧手機、智慧穿戴	Nubia net:192.168.0.0/16
OPPO	智慧手機、智慧穿戴、智慧耳機	OPPO net:192.168.0.0/16
REALME (真我)	智慧手機、智慧穿戴、智慧耳機、智慧電視	REALME net:192.168.0.0/16
SUGAR	智慧手機(IoT 設備較少)	SUGAR net:192.168.0.0/16
Tenda (騰達)	路由器、無線延伸器、交換器、Mesh網路系統	Tenda net:192.168.0.0/16
TotoLink	路由器、無線延伸器、網路攝影機	TotoLink net:192.168.0.0/16

Shodan搜尋 –大陸廠牌資通訊IoT產品 (常見/疑似)

被視為大陸廠牌資通訊產品	常見的IOT類型	語法參考
TP-Link (普聯)	路由器 Mesh 網路系統 智慧燈泡 智慧插座 網路攝影機	TP-Link net:192.168.0.0/16
ZTE (中興通訊)	路由器 智慧手機 5G CPE 智慧家居設備	zte net:192.168.0.0/16
泛學科技 (Panlearn)	線上教學平台(非典型 IoT 設備 無硬體產品)	Panlearn net:192.168.0.0/16

- 以上表格僅供參考，有時品牌名稱並不會直接呈現出來，或是使用其他特徵來顯示。
- 其他廠商可能類似名稱會被搜尋到，搜尋的結果會需要**再次驗證**。

參考資料：
https://inforsec.nutc.edu.tw/p/404-1027-110861.php

建議措施與結論

IP分享器、印表管理介面與 ftp 匿名登入

- 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。

大陸廠牌資通訊產品

- 依據 行政院秘書長109年12月18日院臺護長字第1090201804A號函 規定，**禁止使用及採購大陸廠牌資通訊產品（含軟體、硬體及服務）。**
- 依據 行政院112年6月20日院授數資安字第1121000202號函 及 行政院113年12月31日院授數資安字第1131000727號函 說明，重申各公務機關使用資通訊產品原則：
  - 若因業務需求且無其他替代方案，**應具體敘明理由，並經機關資通安全長及其上級機關資通安全長逐級核可，函報資通安全管理法主管機關（數位發展部）核定**
  - 於汰換前則應有適當之配套措施或相應作為，例如：停用（封存）、使用但不與公務網路介接，或擬訂其他適 當配套管制措施

Thank You !

Q & A