區網會議

資安案例分享

2025/12/30

目 錄

醫院遭CrazyHunter勒索軟體攻擊

前言

馬偕醫院傳出遭CrazyHunter勒索軟體持續攻擊，衛福部與資安署已成立快速應變小組協助因應

今日（11日）傳出國內馬偕醫院遭受勒索軟體Crazy Hunter勒索軟體的事件，衛生福利部資訊處處長李建璋表示確有此事，這次攻擊已經連續兩日，甚至揚言今日傍晚將持續對醫院發動攻擊。在因應上，衛福部已與資安署合作成立快速反應小組，進駐馬偕醫院協助應對。馬偕醫院亦表示，這次事件只有影響北淡兩區急診室

文/ 羅正漢 | 2025-02-11 發表

讚 184 分享

參考資料：
https://www.ithome.com.tw/news/167318
https://www.ithome.com.tw/news/167327

Prince Ransomware

Crazy Hunter Ransomware 為 Prince Ransomware 的進化版本，
加密後會將檔案副檔名加上 .hunter，並留下「Decryption Instructions.txt」，
聯絡 EMAIL 為「attack-tw1337@proton.me」

Prince Ransomware 的說明如下:

```
---------- Ransomware ----------
Your files have been encrypted using Prince Ransomware!
They can only be decrypted by paying us a ransom in cryptocurrency.


Encrypted files have the .prince extension.
IMPORTANT: Do not modify or rename encrypted files, as they may become
unrecoverable.


Contact us at the following email address to discuss payment.
example@airmail.cc
Your ID: BODUGSSVTKHZYASW
---------- Ransomware ----------
```

參考資料：
中華資安報告
圖片來源：
https://www.cyclonis.com/zh-hans/remove-prince-ransomware/

事件說明

2025/02/09 (日)

- 馬偕醫院遭受勒索軟體攻擊，該院立即啟動應變機制、通報衛福部H-ISAC、向調查局臺北市調查處報案。

2025/02/10 (一)

- 馬偕醫院再度遭受勒索軟體攻擊。

2025/02/11 (二)

- H-ISAC發布警訊：防範CrazyHunter這支勒索軟體，並說明已知攻擊路徑為AD主機並派送惡意程式。
- 衛福部與資安署合作成立快速反應小組，進駐馬偕醫院。

後續因應措施

- 有些醫院可能因為資源關係，還沒有部署EDR產品，又或是仍使用老舊缺乏安全更新的作業系統，因此衛福部有協調廠商（微軟）提供2到3個月的免費試用，來補強駭客攻擊的行為偵測與攔阻，暫時因應危險 (https://hisac.nat.gov.tw/news?266)
- 衛福部有提供入侵偵測指標（IoC），讓其他醫院可識別攻擊是否已經發生或正在進行。

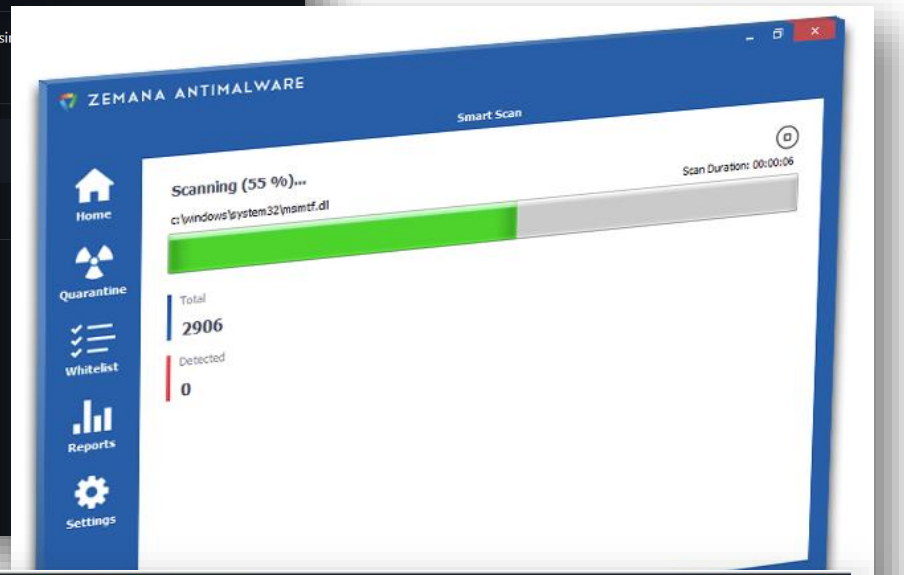
攻擊路徑分析

- **初始入侵**
  - 鎖定AD透過弱密碼嘗試取得帳號權限
  (中華資安報告中研判，攻擊者初始存取點為網頁伺服器等外部可存取之服務)

- **橫向擴散**
  - SharpGPOAbuse
  - 透過GPO發送惡意程式

- **權限提升**
  - 攻擊者採用 **BYOVD（Bring-Your-Own-Vulnerable-Driver）提權攻擊技術**
  - 在端點安裝 Zemana Driver (zam64.sys)，利用有漏洞的合法驅動程式提升權限

- **執行加密**
  - 執行相關惡意程式加密檔案
  - (1)bb.exe，(2)crazyhunter.exe，(3)crazyhunter.sys，(4)zam64.sys，(5)go3.exe，(6)go…



圖片來源：
中華資安報告 中華資安國際 CHT Security
https://github.com/FSecureLABS/SharpGPOAbuse
https://zemana.com/us/antimalware.html

建議處理措施(Windows)

- 開啟Microsoft易受攻擊的驅動程式封鎖清單。

```
    <FileAttrib ID="ID_FILEATTRIB_WCPU" FriendlyName="WCPU\159e7c5a12157af92e0d14a0d3ea1
    <FileAttrib ID="ID_FILEATTRIB_WINKERNEXP" FriendlyName="WindowsKernelExplorer.sys\45
    <FileAttrib ID="ID_FILEATTRIB_WINRING0" FriendlyName="WinRing0.sys" FileName="WinRin
    <FileAttrib ID="ID_FILEATTRIB_WIRWADRV" FriendlyName="Winstron wirwadrv\d8fc8e3a1348
    <FileAttrib ID="ID_FILEATTRIB_WISEUNLO" FriendlyName="WiseUnlo FileAttribute" FileNa
    <FileAttrib ID="ID_FILEATTRIB_WNBIOS" FriendlyName="wnbios.sys\530d9223ec7e4123532a4
    <FileAttrib ID="ID_FILEATTRIB_ZAM_1" FriendlyName="Zemana ZAM\a3908b3fa59c0fc7600ff8
    <FileAttrib ID="ID_FILEATTRIB_ZAM_2" FriendlyName="Zemana Zam\036c1151a30a9c25afc961
    <FileAttrib ID="ID_FILEATTRIB_ZAM_3" FriendlyName="Zemana Zam\0aa79d4c5c3baca0aee095
    <FileAttrib ID="ID_FILEATTRIB_ZAM_4" FriendlyName="Zemana Zam\2b34ca35bd4f61d8e1d62b
    <FileAttrib ID="ID_FILEATTRIB_ZAM_5" FriendlyName="Zemana Zam\c02eabc2e096f00e6e46fb
    <FileAttrib ID="ID_FILEATTRIB_ZAM_6" FriendlyName="Zemana Zam\c3a2dade7d95085d5af4bf
  </FileRules>
  <!--Signers-->
  <Signers>
    <Signer ID="ID_SIGNER_VERISIGN_2010" Name="VeriSign Class 3 Code Signing 2010 CA">
      <CertRoot Type="TBS" Value="4843A82ED3B1F2BFBEE9671960E1940C942F688D" />
```

Windows官方說明：
https://learn.microsoft.com/zh-tw/windows/security/application-security/application-control/app-control-for-business/design/microsoft-recommended-driver-block-rules

建議處理措施

- 衛福部提供以下 IoC 參考

檔案名稱	SHA256 Hash
av-1m.exe	EE854E9F98D0DF34C34551819889336C16B9BFE76E391356CB17B55D59CF28CF
av.exe	3B2081042038C870B1A52C5D5BE965B03B8DD1C2E6D1B56E5EBB7CF3C157138D
bb.exe	2CC975FDB21F6DD20775AA52C7B3DB6866C50761E22338B08FFC7F7748B2ACAA
crazyhunter.exe	F72C03D37DB77E8C6959B293CE81D009BF1C85F7D3BDAA4F873D3241833C146B
crazyhunter.sys	5316060745271723C9934047155DAE95A3920CB6343CA08C93531E1C235861BA
go.exe	754D5C0C494099B72C050E745DDE45EE4F6195C1F559A0F3A0FDDBA353004DB6
go2.exe	983F5346756D61FEC35DF3E6E773FF43973EB96AABAA8094DCBFB5CA17821C81
go3.exe	F72C03D37DB77E8C6959B293CE81D009BF1C85F7D3BDAA4F873D3241833C146B
ru.bat	15160416EC919E0B1A9F2C0DC8D8DC044F696B5B4F94A73EC2AC9D61DBC98D32
ru.bat	731906E699ADDC79E674AB5713C44B917B35CB1EABF11B94C0E9AD954CB1C666
zam64.sys	2BBC6B9DD5E6D0327250B32305BE20C89B19B56D33A096522EE33F22D8C82FF1
zam64.sys	BDF05106F456EE56F97D3EE08E9548C575FC3188AC15C5CE00492E4378045825
ta.bat	527ED180062E2D92B17FF72EA546BB5F8A85AD8B495E5B0C08B6637B9998ACF2
CrazeHunter.zip	D202B3E3E55DF4E424F497BA864AB772BAAF2B8FE10B578C640477F8A8A8610C

建議處理措施

- 資安業者奧義智慧提供以下 IoC 參考

檔案名稱	MD5
aa.exe / cc.exe	7f05a928c77cb87ffb510168c1b0b11b
bb.exe	9fe3322dd4fc35d1ed510bf715dae814
hunter.exe	5e560ea46fa48188cc8768c7e03294d0
crazyhunter.exe	6a70c22a5778eaa433b6ce44513068da
crazyhunter.sys	906e89f6eb39919c6d12a660b68ae81f
file.exe	b7a812586c037ca8d41968842a211b8a
go.exe	ca257aaa1ded22ca22086b9e95cb456d
go2.exe	da1a93627cec6665ae28baaf23ff27c5
zam64.sys	2a3ce41bb2a7894d939fbd1b20dae5a0
gpo.exe	9e45ab7d2d942a575b2f902cccfb3839
ru.bat	f45cc69f74f75a707a02d26ccd912845

大學遭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

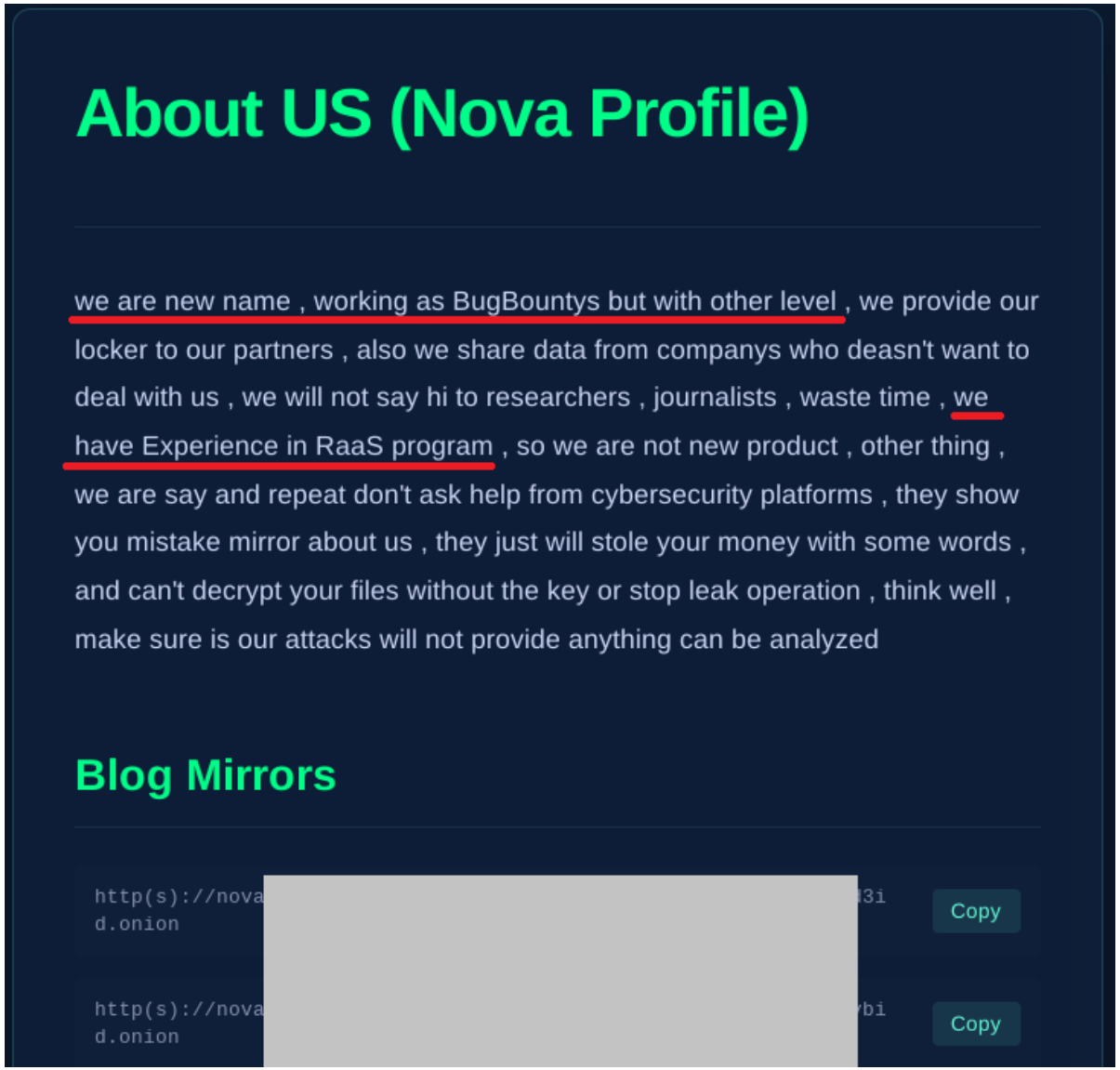
Nova是誰?

- 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：
竣盟科技
https://blog.billows.com.tw/?p=3766&fbclid=IwQ0xDSwLASQpleHRuA2FlbQIxMQABHisfRAccyv48fTqJDf1y5__jU_kskAGFPtRModYqyL32D6fAq0KbmHKX5BXY_aem_Au2X2YhCuni7V4pj3Tl3HQ
CYJAX
https://www.cyjax.com/resources/blog/araastocracy-ralord-ransomware-emerges-with-new-dls/

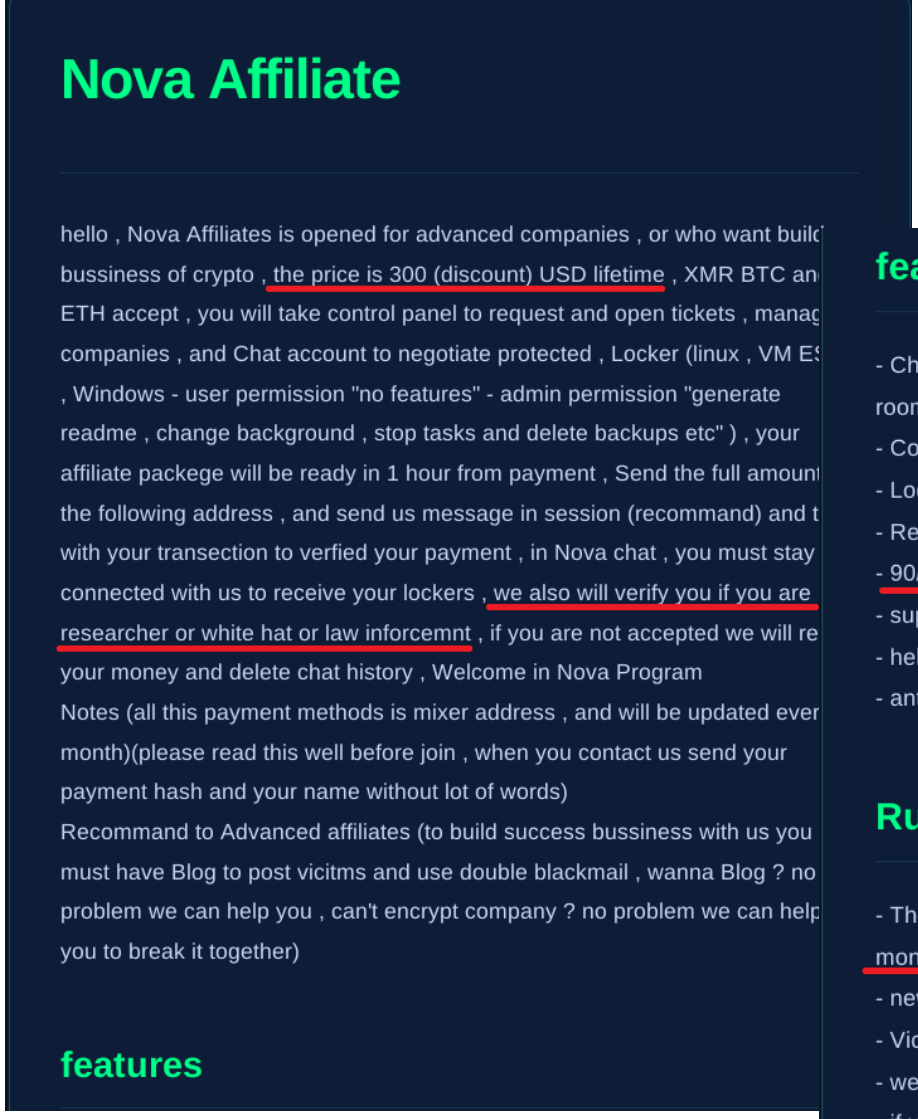
Nova是誰?

- 自我介紹說明 Nova 為新的名稱，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，這可能表明該組織來自使用俄語的國家。



Nova提供的服務

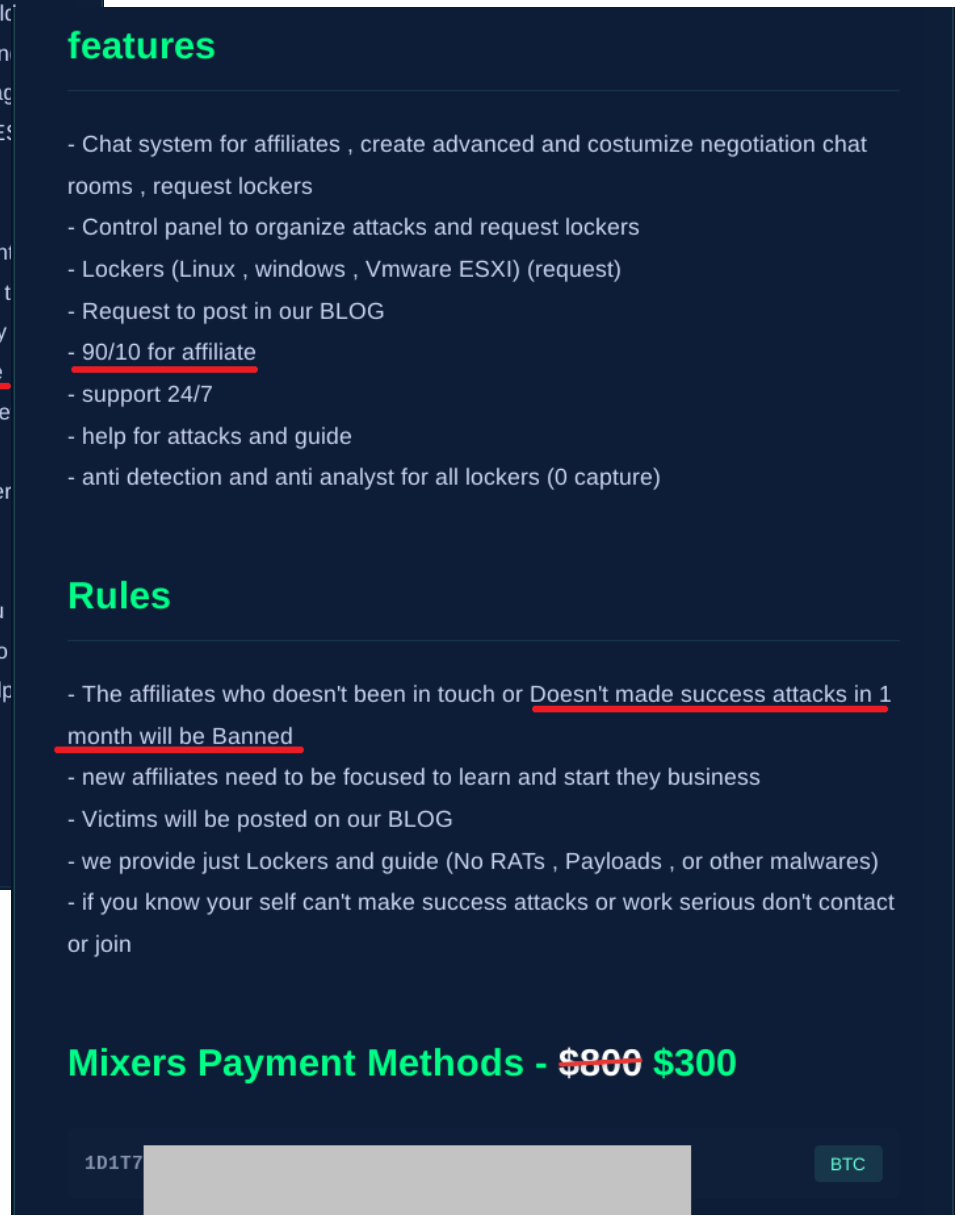
- 開放加盟Nova，目前優惠300美金(終身)。
- Nova會驗證身分，拒絕資安研究員、白帽駭客、執法人員。
- 90/10 for affiliate
  收到贖金後，加盟者可獲得90%利潤，Nova獲得10%利潤。
- 一個月內未攻擊成功的加盟者，會被Nova封鎖。



Nova Affiliate

hello , Nova Affiliates is opened for advanced companies , or who want build 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 ES , 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 amount 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



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

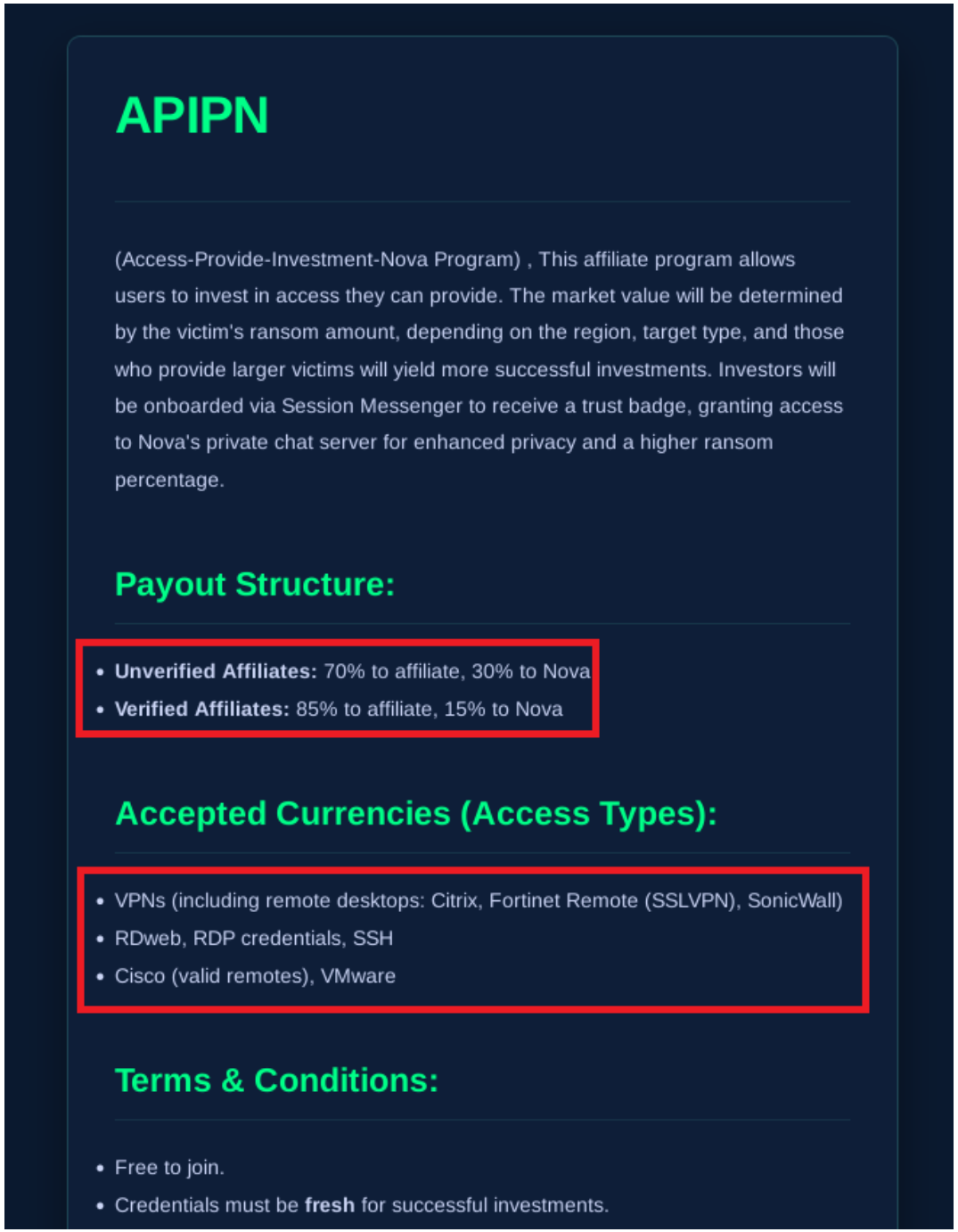
1D1T7 BTC

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。

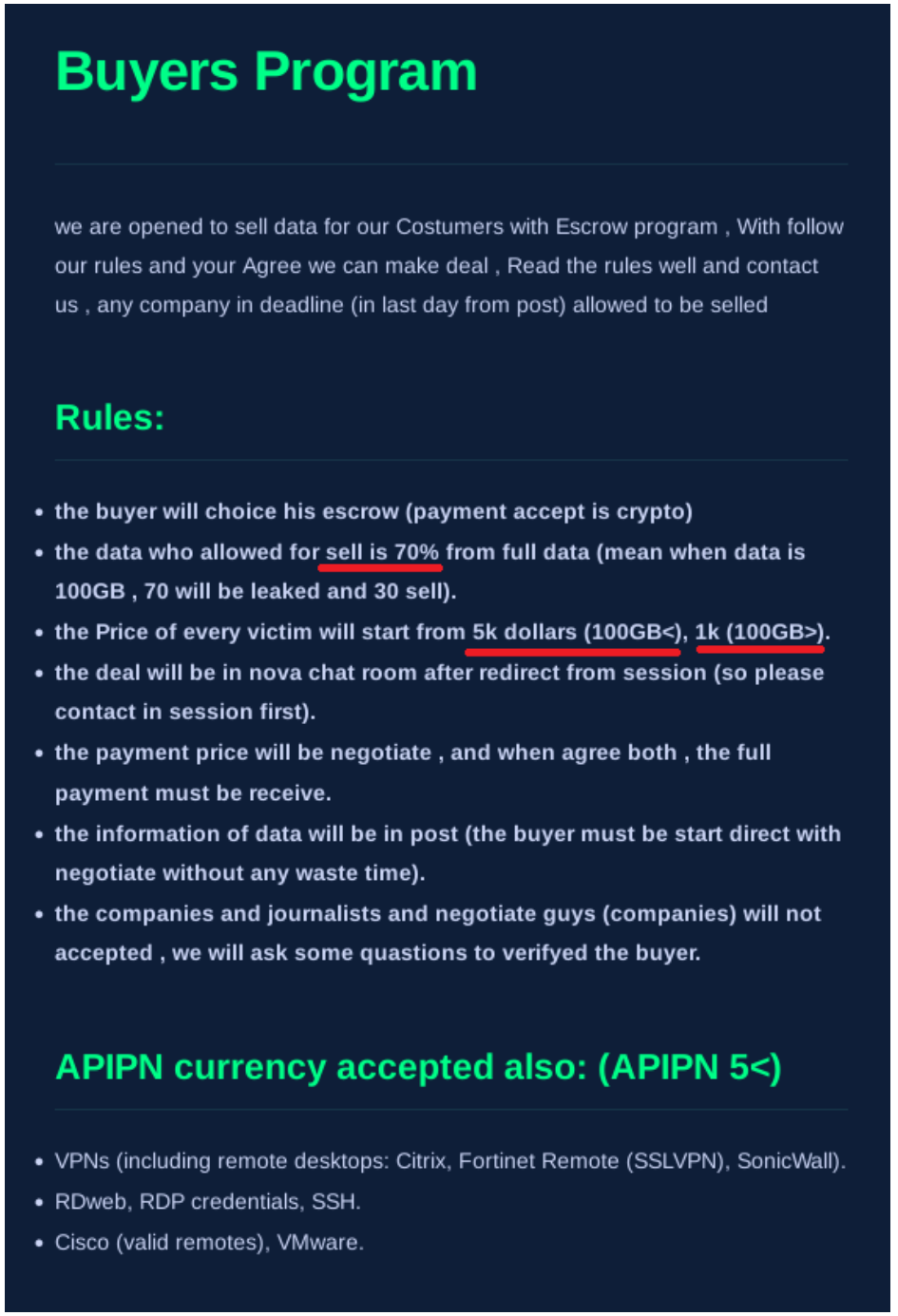
- 收到贖金後，
  未驗證的會員獲得70%利潤，Nova獲得30%利潤。
  已驗證的會員獲得85%利潤，Nova獲得15%利潤
  (已驗證的條件需提供15個以上憑證，及可以順利登入)。

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

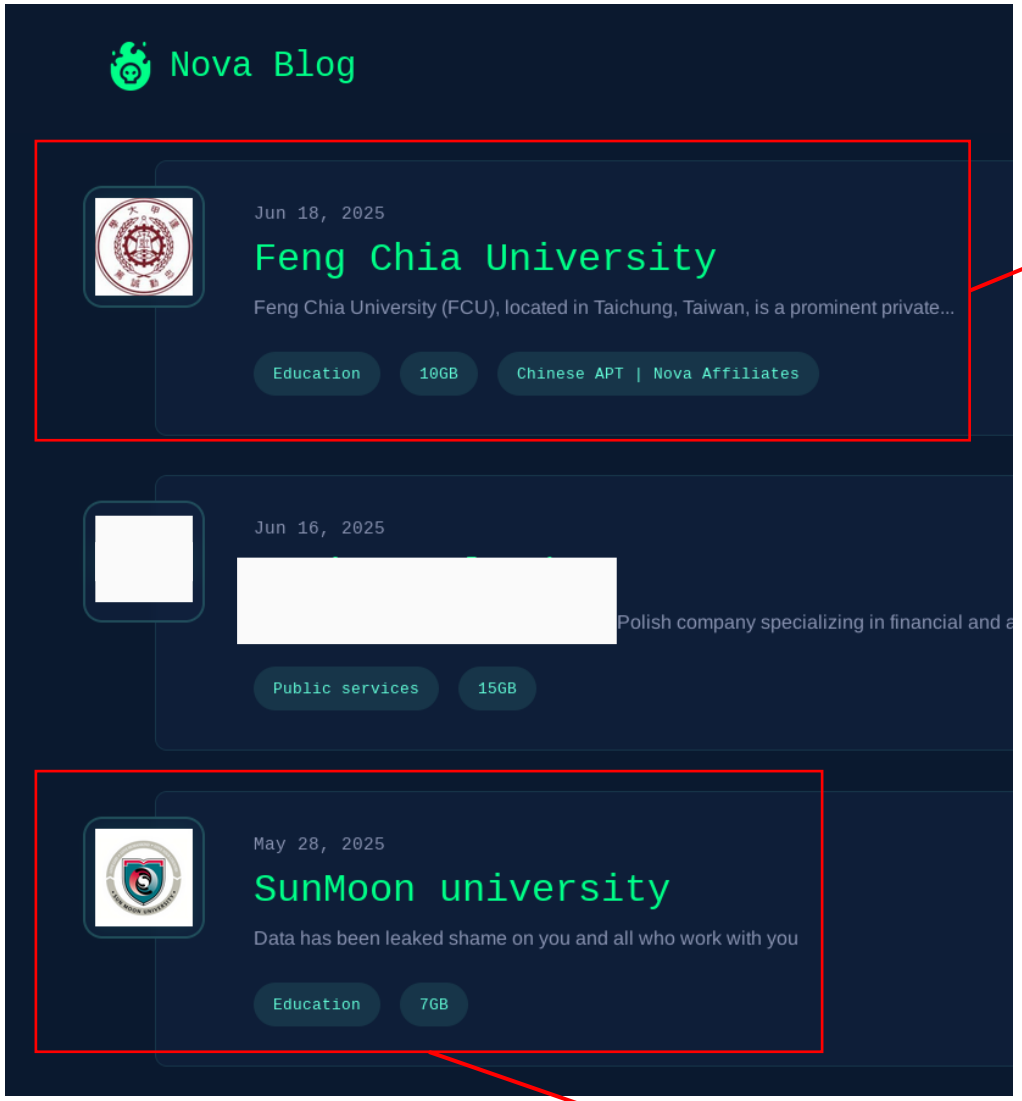


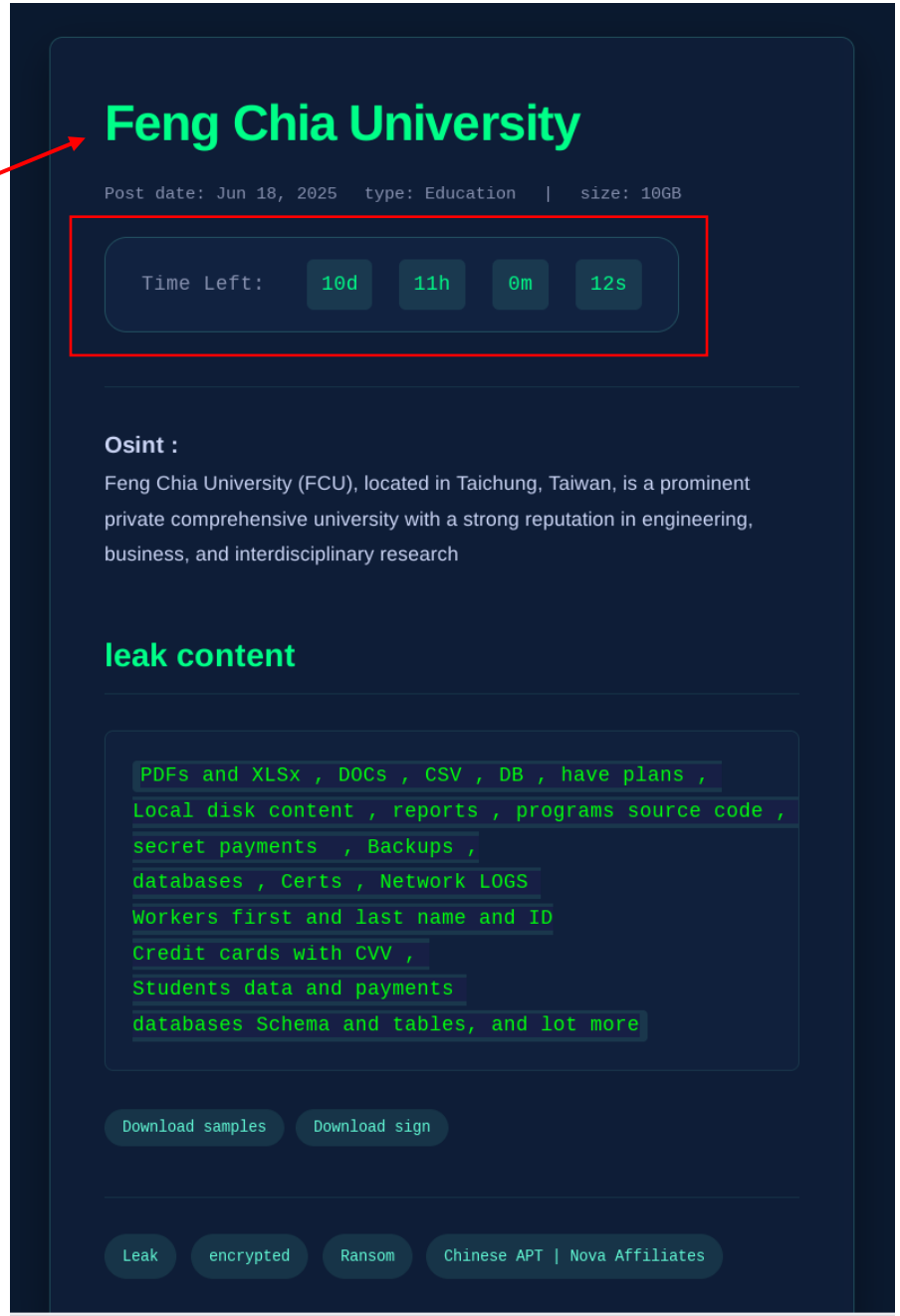
Nova提供的服務

- 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



Nova勒索公告平台

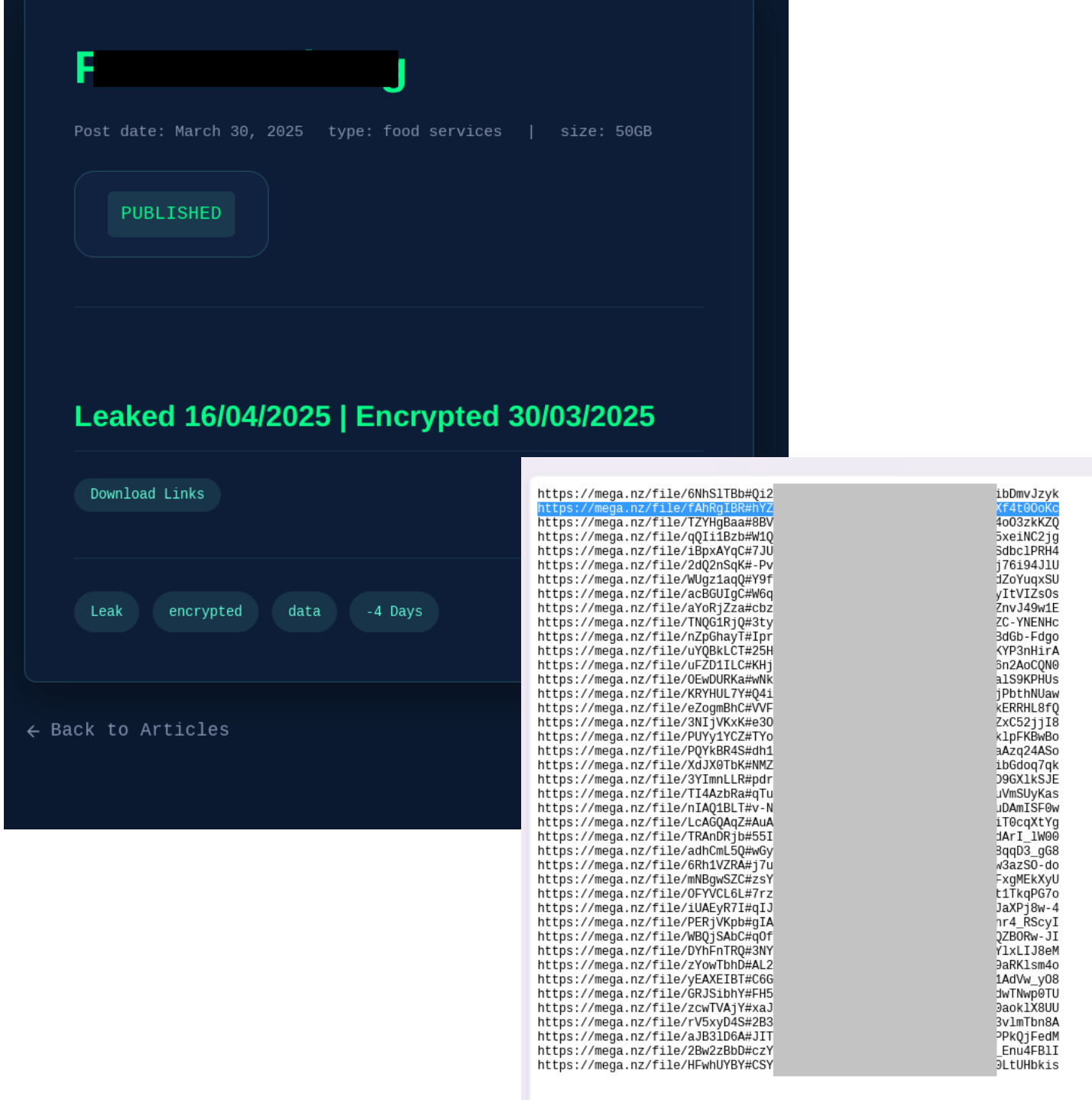




- 南韓顯文大學資料已被公開

Nova勒索公告平台

- 台灣某知名餐飲業者的資料已被公開。
- 檔案下載連結已被公布。



Nova勒索公告平台

合約條文 - 便當協議事項 (2/5)

- 按時送達甲方訂購人所屬[redacted]**指定地點**，不得耽誤。（準時送達）
- 甲方顧客食用便當，若發現有導致疑似食物中毒跡象，並經衛生單位鑑定屬實時，應由乙方負責醫療、復原、損害賠償並負法律上一切民事、刑事責任；甲方得終止契約並沒收履約保證金 **50,000 元**。

[redacted]便當([redacted]年[redacted])

門市	門市回報金額	①[redacted]上期未入金額	②[redacted]立帳金額	立帳金額合計 ①+②+③	差異	立帳金額調整	列下期金額
A[redacted]	4[redacted]	[redacted]	4[redacted]	4[redacted]	[redacted]	[redacted]	2[redacted]
A[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
A[redacted]	1[redacted]	[redacted]	1[redacted]	1[redacted]	[redacted]	[redacted]	1[redacted]
A[redacted]	1[redacted]	[redacted]	1[redacted]	1[redacted]	[redacted]	-[redacted]	[redacted]
A[redacted]	5[redacted]	[redacted]	[redacted]	5[redacted]	[redacted]	[redacted]	[redacted]
A[redacted]	2[redacted]	[redacted]	2[redacted]	2[redacted]	[redacted]	[redacted]	2[redacted]
A[redacted]	1[redacted]	[redacted]	1[redacted]	1[redacted]	[redacted]	[redacted]	1[redacted]
A[redacted]	[redacted]	-1	[redacted]	-[redacted]	[redacted]	[redacted]	-[redacted]
A[redacted]	5[redacted]	[redacted]	[redacted]	5[redacted]	[redacted]	[redacted]	[redacted]
A[redacted]	5[redacted]	4	[redacted]	1[redacted]	[redacted]	[redacted]	1[redacted]
A[redacted]	7[redacted]	[redacted]	7[redacted]	7[redacted]	-[redacted]	3[redacted]	-[redacted]
A[redacted]	2[redacted]	[redacted]	2[redacted]	2[redacted]	[redacted]	[redacted]	[redacted]
A[redacted]	1[redacted]	[redacted]	1[redacted]	1[redacted]	[redacted]	[redacted]	[redacted]
A[redacted]	5[redacted]	[redacted]	5[redacted]	5[redacted]	[redacted]	-[redacted]	[redacted]
A[redacted]	1[redacted]	[redacted]	1[redacted]	1[redacted]	[redacted]	[redacted]	[redacted]
A[redacted]	4[redacted]	[redacted]	4[redacted]	4[redacted]	[redacted]	[redacted]	-1[redacted]
A[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
A[redacted]	1[redacted]	[redacted]	1[redacted]	1[redacted]	[redacted]	[redacted]	1[redacted]
A[redacted]	1[redacted]	[redacted]	1[redacted]	1[redacted]	[redacted]	[redacted]	[redacted]
A[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	-[redacted]
A[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
A[redacted]	1[redacted]	4	1[redacted]	1[redacted]	1	-1	7[redacted]
A[redacted]	1[redacted]	[redacted]	1[redacted]	1[redacted]	[redacted]	[redacted]	[redacted]
A[redacted]	5[redacted]	[redacted]	5[redacted]	5[redacted]	[redacted]	-[redacted]	[redacted]
A[redacted]	5[redacted]	[redacted]	5[redacted]	5[redacted]	[redacted]	[redacted]	[redacted]
A[redacted]	2[redacted]	[redacted]	2[redacted]	2[redacted]	[redacted]	-[redacted]	[redacted]
總計	7[redacted]	8	7[redacted]	7[redacted]	[redacted]	-2	1[redacted]

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。

SEO Poisoning

SEO Poisoning 搜尋引擎最佳化中毒

- 在google搜尋欄輸入：
  site:edu.tw SLOT THAILAND (泰國線上老虎機)

  結果會出現許多學校的網站，但進去是正常的內容，通常是google快取的問題，需再跟google申請移除。

- 教育部接獲學校反映，利用google hacking(dorking)技術，會查詢到不相關或不當資訊出現。

- 北區ASOC協助檢測學網網站及開單通報。

- SEO Poisoning 通常目的是以下4點，
  1. 引導受害者前往惡意或詐騙網站
  跳轉釣魚頁面、假更新、投資詐騙、賭博等。
  2. 散佈惡意程式
  透過假下載、假安裝包或跳轉頁面植入木馬、勒索軟體、Infostealer。
  3. 操控搜尋排名(黑帽 SEO)
  利用被駭網站提高攻擊者網站的權重與曝光度。
  4. 流量變現
  把搜尋流量導向廣告農場、賭博站、垃圾站，以賺取點擊收益。

SEO Poisoning 搜尋引擎最佳化中毒

3. 如確認已遭到 SEO 中毒攻擊（SEO Poisoning），即可至 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。(請參考附錄二)
4. 在符合單位政策的情況下，可在 robots.txt 加上不允許搜尋引擎檢索站內搜尋結果之指令，也可在站內每個搜尋結果加上<meta noindex>，來避免被搜尋引擎所檢索。(提醒:若單位在 robots.txt 設定，可能造成學校於 Google 上檢索不到，降低學校被搜尋的可能性)。

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))。

- 2025/11/28北區ASOC開單通知4所學校，及提供TACERT的Google移除網址說明，給學校參考移除方式。

➢ TACERT提供的移除網址部分說明

物聯網設備防護與資安案例

IoT搜尋引擎

- **Shodan(https://www.shodan.io/)**
- Censys(https://censys.com/)
- Fofa(https://fofa.info/)
- ZoomEye(https://www.zoomeye.ai/)

IoT搜尋引擎
Shodan學術帳號

- 申請一般帳號

學術升級

Shodan 為使用學術電子郵件地址（例如以 結尾的地址等）註冊的用戶提供免費的會員升級服務，學術會員資格包括以下內容： `.edu` `.ac.uk`

- 能夠監控最多 16 個 IP
- 每月 100 個查詢積分
- 每月 100 次掃描積分
- 訪問Shodan 地圖和Shodan 圖像
- `vuln` 可以在網站上使用過濾器

https://help.shodan.io/the-basics/academic-upgrade

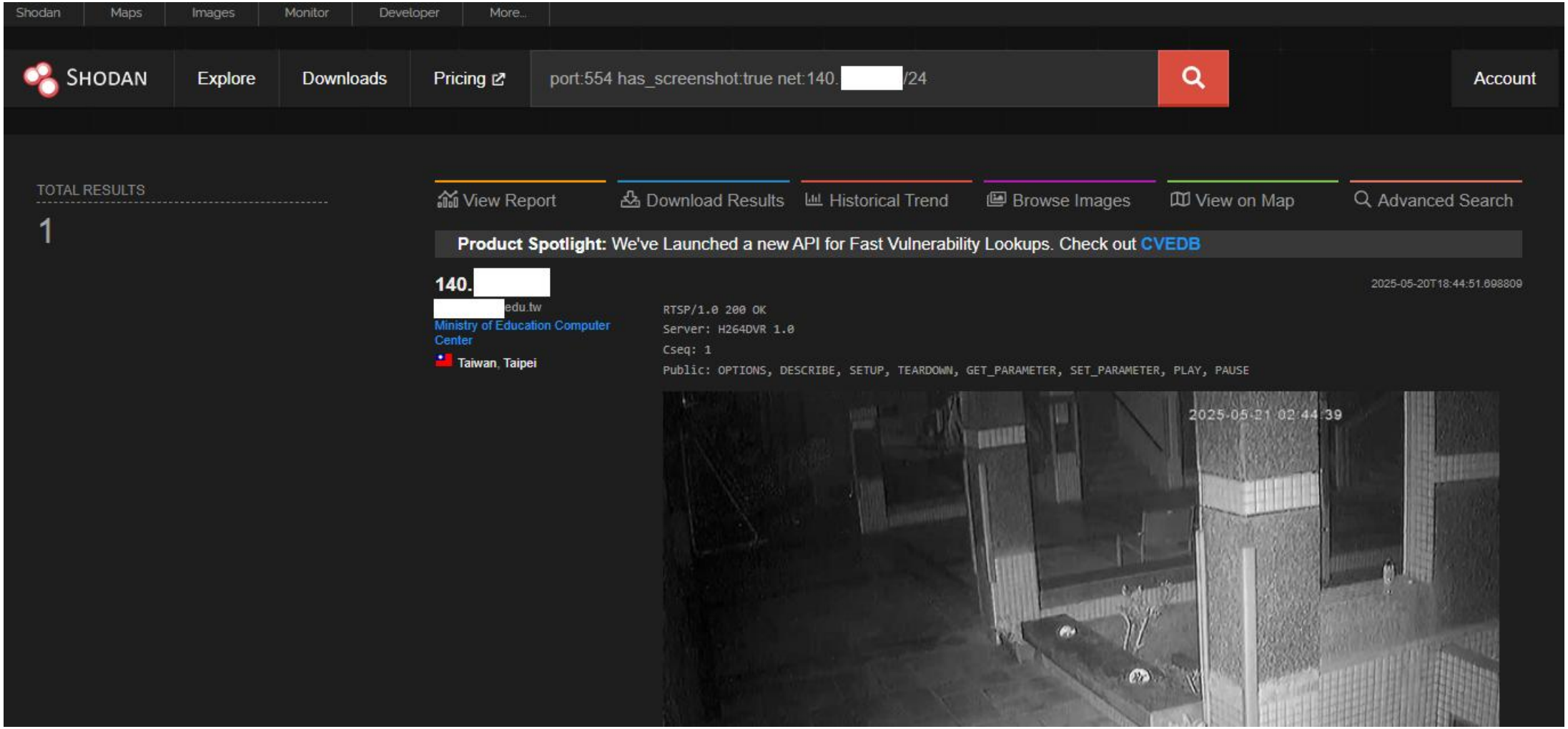
IoT搜尋引擎
Shodan常用查詢參數 x 常用連接埠

參數	說明	範例
net	IP位置或網段	net:123.23.1.0/24
port	連接埠	port:21
product	作業系統/軟體名稱	product:windows
country	國家	country:tw
city	城市	city:"Taipei"
org	組織或公司	org:google
hostname	主機名稱	hostname:www.edu.tw
org	組織或公司	org:google
http.title	網站標題	http.title:"hacked by"
vuln	漏洞編號	vuln:CVE-2014-0160

連接埠	說明
21	FTP
80 443 8080 8443 5000 5001	HTTP/HTTPS 管理介面/資訊頁
554	RTSP
22	SSH
23	TELNET
515	LPD
631	IPP
9100	PDL
161	SNMP
1900	UPnP

https://www.shodan.io/search/examples

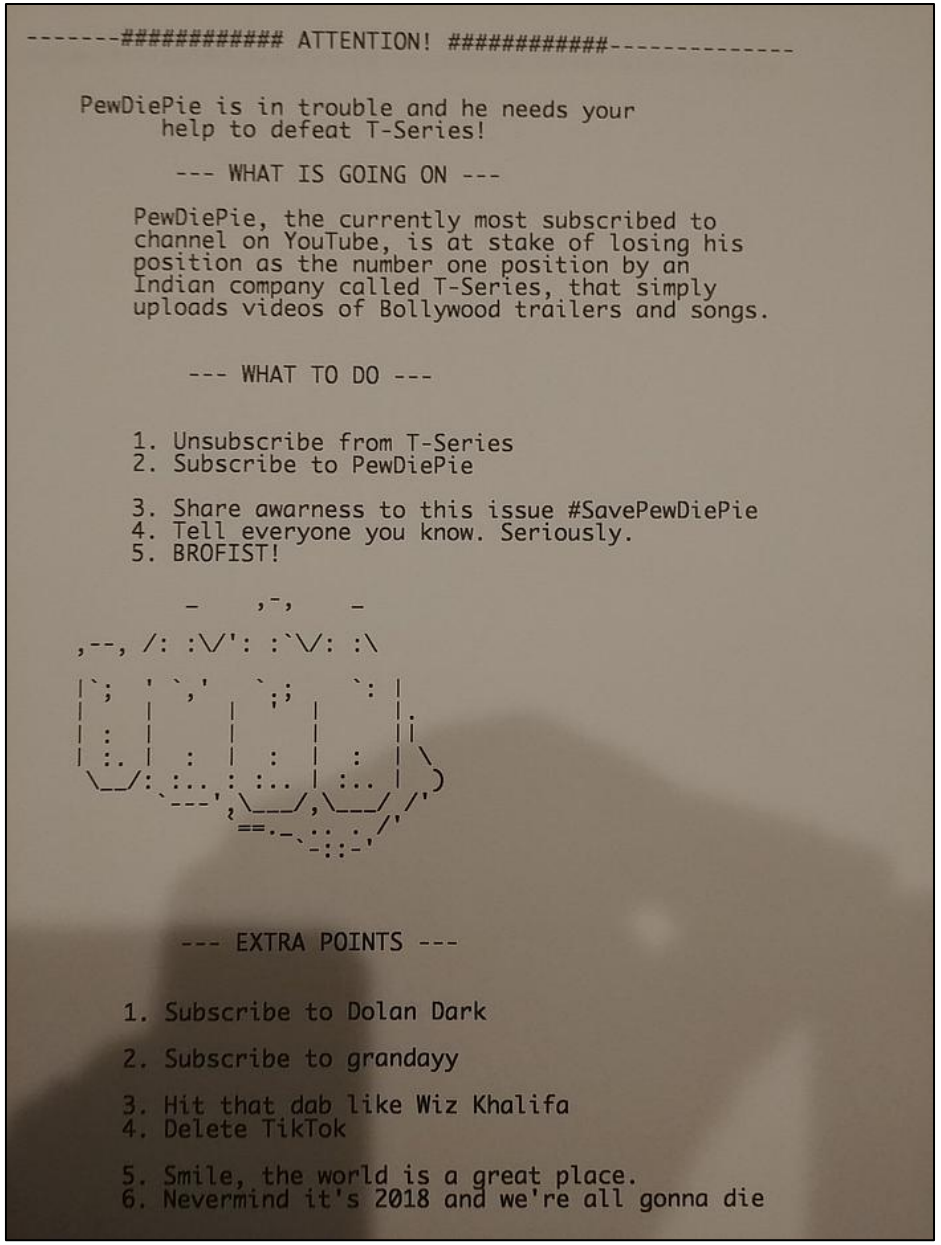
IoT搜尋引擎
Shodan-攝影機/影像監控設備(IP Cam)



port:554 has_screenshot:true net:140.x.x.0/24

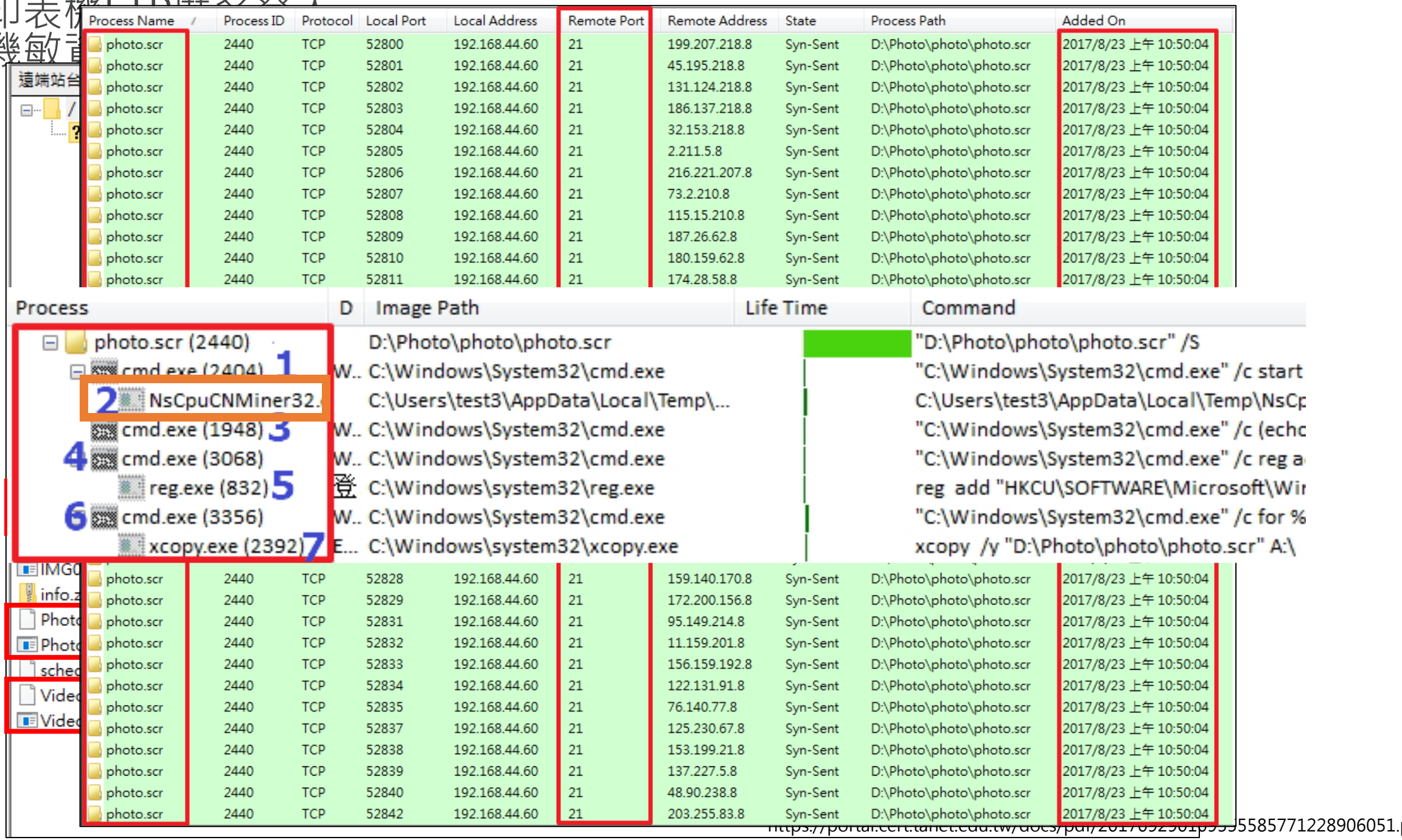
https://www.shodan.io/

印表機駭客



https://shadowmaster98.medium.com/printer-hacking-101-b4faf4f3fcdc
https://www.ithome.com.tw/news/127458

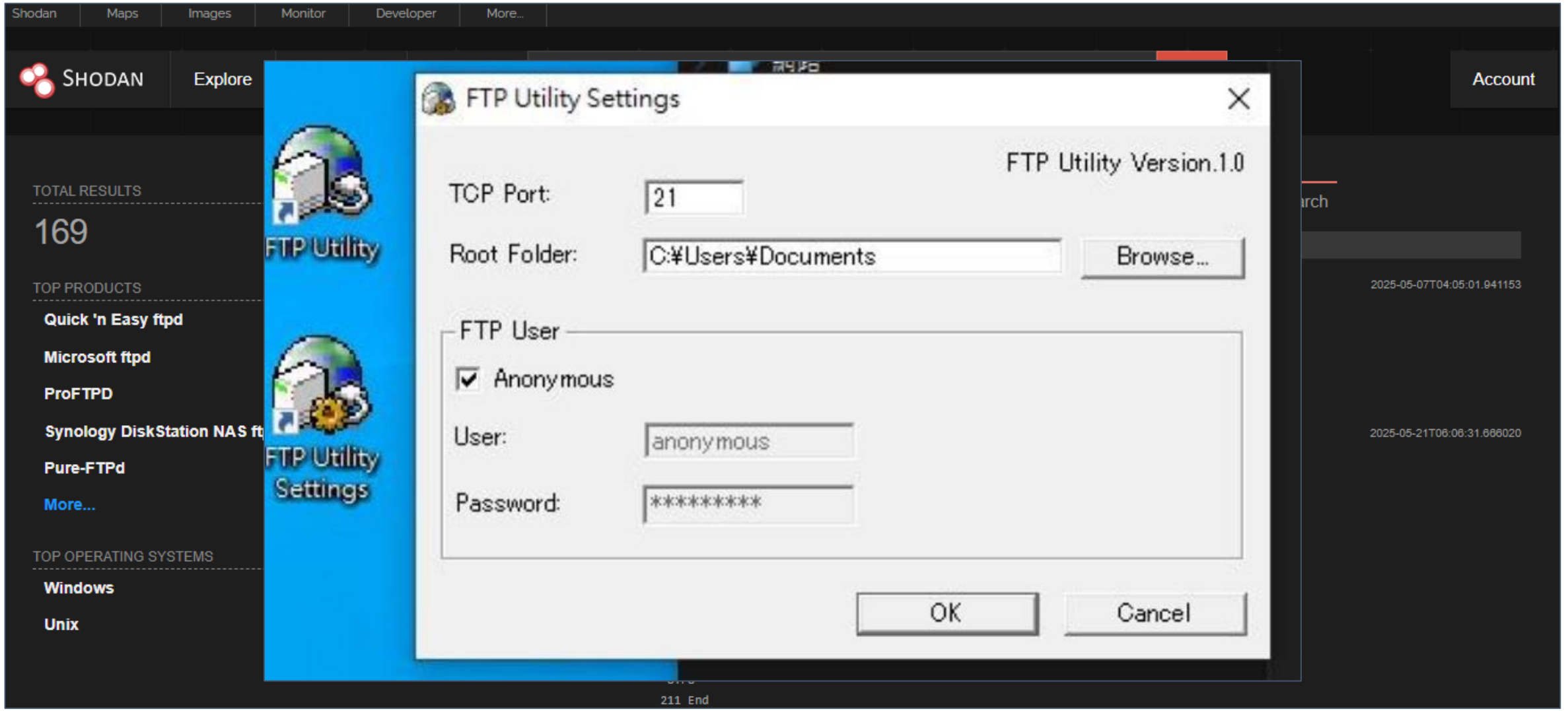
印表機FTP歷名登入
機敏資



Process Name	Process ID	Protocol	Local Port	Local Address	Remote Port	Remote Address	State	Process Path	Added On
photo.scr	2440	TCP	52800	192.168.44.60	21	199.207.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52801	192.168.44.60	21	45.195.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52802	192.168.44.60	21	131.124.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52803	192.168.44.60	21	186.137.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52804	192.168.44.60	21	32.153.218.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52805	192.168.44.60	21	2.211.5.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52806	192.168.44.60	21	216.221.207.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52807	192.168.44.60	21	73.2.210.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52808	192.168.44.60	21	115.15.210.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52809	192.168.44.60	21	187.26.62.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52810	192.168.44.60	21	180.159.62.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52811	192.168.44.60	21	174.28.58.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52828	192.168.44.60	21	159.140.170.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52829	192.168.44.60	21	172.200.156.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52831	192.168.44.60	21	95.149.214.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52832	192.168.44.60	21	11.159.201.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52833	192.168.44.60	21	156.159.192.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52834	192.168.44.60	21	122.131.91.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52835	192.168.44.60	21	76.140.77.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52837	192.168.44.60	21	125.230.67.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52838	192.168.44.60	21	153.199.21.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52839	192.168.44.60	21	137.227.5.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52840	192.168.44.60	21	48.90.238.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04
photo.scr	2440	TCP	52842	192.168.44.60	21	203.255.83.8	Syn-Sent	D:\Photo\photo\photo.scr	2017/8/23 上午 10:50:04

Process	D	Image Path	Life Time	Command
photo.scr (2440)		D:\Photo\photo\photo.scr		"D:\Photo\photo\photo.scr" /S
1 cmd.exe (2404)	W..	C:\Windows\System32\cmd.exe		"C:\Windows\System32\cmd.exe" /c start
2 NsCpuCNMiner32.		C:\Users\test3\AppData\Local\Temp\...		C:\Users\test3\AppData\Local\Temp\NsCp
3 cmd.exe (1948)	W..	C:\Windows\System32\cmd.exe		"C:\Windows\System32\cmd.exe" /c (echc
4 cmd.exe (3068)	W..	C:\Windows\System32\cmd.exe		"C:\Windows\System32\cmd.exe" /c reg a
5 reg.exe (832)	登	C:\Windows\system32\reg.exe		reg add "HKCU\SOFTWARE\Microsoft\Wir
6 cmd.exe (3356)	W..	C:\Windows\System32\cmd.exe		"C:\Windows\System32\cmd.exe" /c for %
7 xcopy.exe (2392)	E...	C:\Windows\system32\xcopy.exe		xcopy /y "D:\Photo\photo\photo.scr" A:\

IoT搜尋引擎
Shodan-FTP檔案傳輸協定



port:21 net:140.x.x.0/16

https://www.shodan.io/
https://www.cc.ntu.edu.tw/chinese/epaper/home/20210620_005705.html

```
Nmap scan report for us[redacted].edu.tw (140.[redacted])
Host is up (0.0025s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 192.168.147.231 is not the same as 140.[redacted]

Nmap scan report for ftp.ntu.edu.tw (140.[redacted])
Host is up (0.0030s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV IP 192.168.110.102 is not the same as 140.[redacted]

Nmap scan report for 140.[redacted]
Host is up (0.0030s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rwxrwxrwx   1 SYSTEM   SYSTEM       5826390 Sep 22  2016 1050922\xA8t\xB0\xC8\xB7|\xC4\xB3\xC4\xB3\xB5{.pdf [NSE: writeable]
| -rwxrwxrwx   1 alicelin alicelin    13536667 May 12 11:47 3.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM       1913258 Oct 18  2013 SCAN20131018163139.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        236733 Nov 13  2013 SCAN20131113101833.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        246973 Nov 13  2013 SCAN20131113101900.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        236733 Nov 13  2013 SCAN20131113101920.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        462686 Nov 13  2013 SCAN20131113101954.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        730272 Nov 13  2013 SCAN20131113102043.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        329566 Nov 13  2013 SCAN20131113102137.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        175293 Nov 13  2013 SCAN20131113102632.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM       1192419 Nov 13  2013 SCAN20131113102658.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM       1018339 Nov 13  2013 SCAN20131113102814.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        935745 Nov 15  2013 SCAN20131115181414.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM       1470245 Nov 19  2013 SCAN20131119115314.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        175293 Dec 20  2013 SCAN20131220151442.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        267454 Dec 30  2013 SCAN20131230165836.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        226494 Dec 30  2013 SCAN20131230165902.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        267455 Dec 30  2013 SCAN20131230175645.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        134333 May 02  2014 SCAN20140502120926.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        720032 May 02  2014 SCAN20140502123746.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM       1470245 May 16  2014 SCAN20140516141624.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        360286 May 16  2014 SCAN20140516154547.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        216253 May 16  2014 SCAN20140516160020.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        216253 May 16  2014 SCAN20140516160047.pdf [NSE: writeable]
| -rwxrwxrwx   1 SYSTEM   SYSTEM        216253 May 16  2014 SCAN20140516160102.pdf [NSE: writeable]
```

nmap.org/

IoT設備攻擊防範建議

- 定時更新軟(韌體)版本
- 加強登入密碼的強度，或啟用多重要素驗證(MFA)驗證機制
- 使用虛擬IP，關閉非必要的連接埠
- 變更或停用不安全的預設設定
- 限制IP連線存取(ACL)，以及嚴格控管帳號權限
- 建議採購包含完整安全檢測之產品

感謝聆聽!