



# 政府機關資安威脅與防護重點

NCCST

行政院國家資通安全會報技術服務中心

110年11月

- 資通安全威脅趨勢與案例分享
  - 全球資通安全威脅趨勢
  - 政府資通安全威脅趨勢
  - 政府資安事件案例分享
- 政府機關資安防護強化重點
  - 落實資安縱深防禦
  - 善用通報應變網站情資分享
- 結論與建議

# 世界經濟論壇2021全球風險調查報告



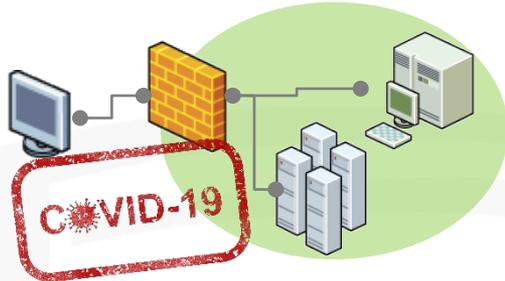
- ### 10大影響風險
1. 傳染病
  2. 緩解氣候變化行動失敗
  3. 大規模殺傷性武器
  4. 生物多樣式喪失
  5. 自然資源危機
  6. 人為環境災害
  7. 民生危機
  8. 極端氣候
  9. 債務危機
  10. 資訊基礎建設破壞(109年排名第6)

- ### 10大可能長期風險
1. 極端氣候
  2. 緩解氣候變化行動失敗
  3. 人為導致的環境災害
  4. 傳染病
  5. 生物多樣式喪失
  6. 數位集權
  7. 數位不平等
  8. 國際關係裂痕
  9. 資安防護失敗
  10. 民生危機

紅色：科技因素  
藍色：新增因子

# 全球資通安全威脅趨勢

- 綜整110年全球資安威脅與相關研究報告，歸納全球資安威脅趨勢



**遠距工作型態  
促使網路攻擊提升**



**勒索軟體攻擊  
風險激增**



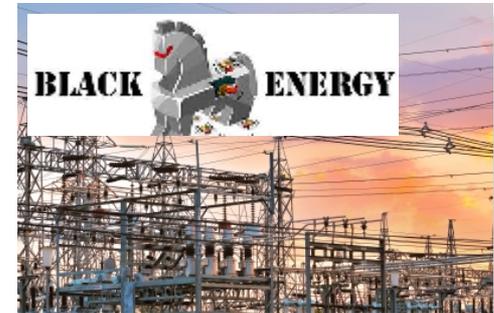
**社交工程手法仍頻繁**



**國家層級駭客  
攻擊仍頻繁**



**資安(訊)供應商持續遭  
駭破壞供應鏈安全**



**關鍵基礎設施  
資安風險倍增**

# 遠距工作型態促使網路攻擊提升



- ENISA Threat Landscape報告<sup>[1]</sup>與資安廠商卡巴斯基之110年APT威脅態勢預測<sup>[2]</sup>指出
  - 居家辦公技術屢遭攻擊，新攻擊媒介將針對企業網路設備(如VPN設備等)與RDP遠端桌面協定攻擊
- 商用軟體Exchange Server產品漏洞也屢遭開採與利用



Alerts and Tips Resources Industrial Control Systems

National Cyber Awareness System > Current Activity > Urgent: Protect Against Active Exploitation of ProxyShell

## Urgent: Protect Against Active Exploitation of ProxyShell Vulnerabilities

美國網路安全及基礎設施安全局(CISA)呼籲使用者進行修補微軟Exchange與Pulse Secure軟體漏洞

National Alerts and Tips System > Alerts > Exploitation of Pulse Connect Secure Vulnerabilities

### Alert (AA21-110A)

Exploitation of Pulse Connect Secure Vulnerabilities

漏洞代號	CVE編號	CVSS Score
Proxy Logon	CVE-2021-26855	9.8 CRITICAL
	CVE-2021-26857	7.8 HIGH
	CVE-2021-26858	7.8 HIGH
	CVE-2021-27065	7.8 HIGH
Proxy Oracle	CVE-2021-31195	8.8 HIGH
	CVE-2021-31196	7.2 HIGH
N/A	CVE-2021-33768	8.0 HIGH
Proxy Shell	CVE-2021-34473	9.8 CRITICAL
	CVE-2021-34523	9.8 CRITICAL
	CVE-2021-31207	7.2 HIGH

微軟Exchange軟體漏洞威脅一覽

資料來源：

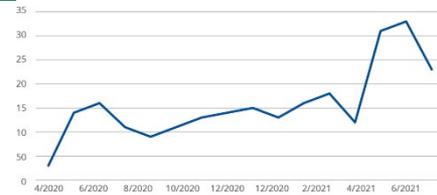
1. ENISA Threat Landscape, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>

2. <https://securelist.com/apt-predictions-for-2021/99387/>

# 勒索軟體攻擊風險激增

- 虛擬貨幣支付應用提升勒索攻擊

- ENISA Threat Landscape報告指出，相關攻擊衍生為勒索軟體即服務(Ransomware-as-a-Service, RaaS)
- 資安業者Sophos<sup>[1]</sup>統計，使用者支付贖金比例由109年26%增加至110年32%



ENISA  
109/4~110/6  
勒索事件統計

- 勒索攻擊轉向目標式攻擊，造成經濟損失、重要資料外洩及重要服務中斷

- 墨爾本醫療網路遭勒索攻擊<sup>[2]</sup>，使醫療人員無法存取相關醫療資訊，導致部分手術停擺
- DarkSide勒索病毒攻擊事件造成負責美國東岸近半數油管運輸的Colonial Pipeline公司主動關閉營業



澳洲醫療網路遭勒索攻擊



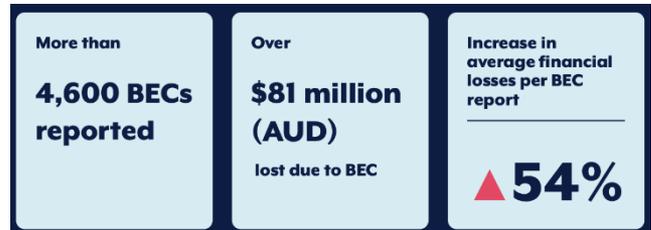
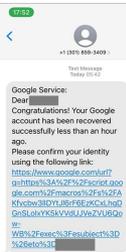
CISA DarkSide事件公告

資料來源：

1. <https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf>
2. <https://www.theage.com.au/national/victoria/staff-unable-to-access-patient-files-after-eastern-health-cyber-attack-20210329-p57eyj.html>

# 社交工程手法仍頻繁

- 社交工程電子郵件攻擊主要包含**釣魚郵件(Phishing)**與**商業電子郵件詐騙(Business E-mail Compromise, BEC)**
- 釣魚郵件利用熱門議題吸引目標，以竊取機敏資訊
  - 澳洲政府於110年偵測發現7,700個COVID-19相關網站
  - 伊朗駭客組織(Charming Kitten, APT35)使用整合SMS簡訊之網路釣魚簡訊手法(Smishing)進行攻擊
- 針對性魚叉式攻擊(Spear-Phishing)與商業電子郵件詐騙常結合域名與網址偽冒行為
  - 依據澳洲ACSC統計，澳洲109~110年共接獲4,600則BEC事件通報
  - 損失8,145萬澳幣，較前年成長15%



資料來源：

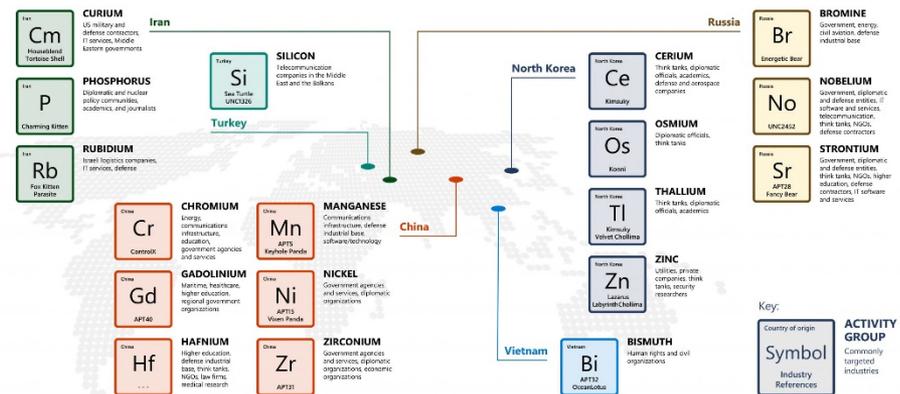
<https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21>

澳洲ACSC 商業電子郵件詐騙統計

# 國家層級駭客攻擊仍頻繁

- 微軟數位防禦報告(Microsoft Digital Defense Report, MDDR)指出，國家型駭客組織主要攻擊目標為美國(46%)、烏克蘭(19%)及英國(9%)
  - 攻擊政府機構(48%)、非政府組織與智庫組織(31%)
  - 駭客組織分布於中國(6)、北韓(4)、俄羅斯(3)及伊朗(3)
  - 中國駭客經常利用零時差漏洞展開攻擊，蒐集情報目的多元
  - 駭客組織Chromium鎖定印度、馬來西亞、蒙古、巴基斯坦及泰國等國，以及針對香港與台灣的社會、經濟及政治議題

Sample Nation-State Actors



資料來源：  
<https://blogs.microsoft.com/on-the-issues/2021/10/07/digital-defense-report-2021/>

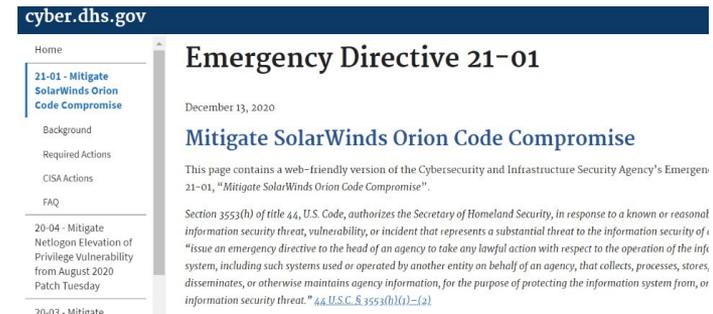
# 資安(訊)供應商遭駭破壞供應鏈安全



- ENISA Threat Landscape報告<sup>[1]</sup>指出，109~110年可確認之APT攻擊共17次，其中供應鏈攻擊超過50%

## – 109年12月SolarWinds事件<sup>[2]</sup>

- 國家級駭客透過SolarWinds平台重大漏洞攻擊美國財政部與商務部及其他民間企業
- 駭客至少潛伏在受駭機構達數月之久，且相關電子郵件長期受到偷窺監視



美國國土安全部要求所有聯邦機構網站關閉SolarWinds相關產品

## – 110年7月IT管理軟體商Kaseya遭駭事件<sup>[3]</sup>

- Kaseya VSA為遠端監控與管理軟體，用於企業管理與託管服務供應商 (Managed Service Provider, MSP)
- Revil駭客組織攻擊事件超過200家美國企業受害，包含30家採用Kaseya VSA軟體的託管服務供應商之客戶



資料來源：

1. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>
2. <https://cyber.dhs.gov/ed/21-01/>
3. <https://www.kaseya.com/potential-attack-on-kaseya-vsa/>

# 關鍵基礎設施資安風險倍增



- 關鍵基礎設施容易遭受具網路存取之工業控制服務
  - 110年2月駭客利用淨水廠IT管理所使用TeamViewer漏洞存取工廠控制系統<sup>[1]</sup>，並更改淨水廠控制系統相關參數至超標數值
  - 110年7月伊朗火車系統遭到入侵<sup>[2]</sup>，火車資訊顯示系統遭竄改造成服務中斷
  - 110年10月伊朗國營石油公司Niopdc傳出因受到網路攻擊<sup>[3]</sup>，近4,000個加油站停止運作，持續數小時才復原



## Following Oldsmar attack, FBI warns about using TeamViewer and Windows 7

An FBI alert sent on Tuesday warns companies about the use of out-of-date Windows 7 systems, poor account passwords, and desktop sharing software TeamViewer.

資料來源：  
<https://www.zdnet.com/article/following-oldsmar-attack-fbi-warns-about-using-teamviewer-and-windows-7/>



Fars News reports that hundreds of trains in #Iran have suddenly been cancelled today, speculating about a cyber attack on railway computer systems.



下午11:14 · 2021年7月9日 · Twitter Web App

資料來源：  
1.<https://www.zdnet.com/article/following-oldsmar-attack-fbi-warns-about-using-teamviewer-and-windows-7/>  
2.<https://www.ithome.com.tw/news/145956>  
3.<https://www.bleepingcomputer.com/news/security/iranian-gas-stations-out-of-service-after-distribution-network-hacked/>

- 資通安全威脅趨勢與案例分享
  - 全球資通安全威脅趨勢
  - 政府資通安全威脅趨勢
  - 政府資安事件案例分享
- 政府機關資安防護強化重點
  - 落實資安縱深防禦
  - 善用通報應變網站情資分享
- 結論與建議

# 政府資通安全威脅趨勢



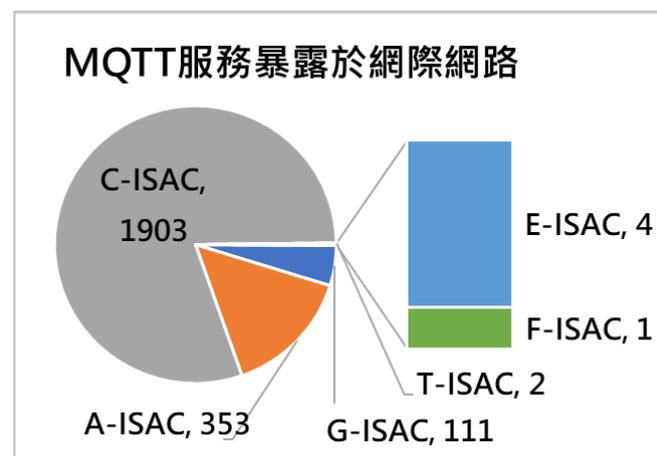
# 工控與物聯網應用衍生資安風險



- 近年來智慧城市、交通及工控聯網應用蓬勃發展
- 部分應用服務暴露於網際網路，存在資安風險

應用類型	應用範例
環境監看	溫度、溼度及空氣品質監測
設備監控	水利設施、太陽能系統狀態監測
工業控制	PLC、HMI及SCADA應用
農業應用	水質、光線照度及冷鏈資訊監測
智慧交通	智慧交通號誌、科技執法
金融服務	金融交易紀錄
居家生活	智慧家電、影音串流及叫車服務
學術研究	實驗室設備監控

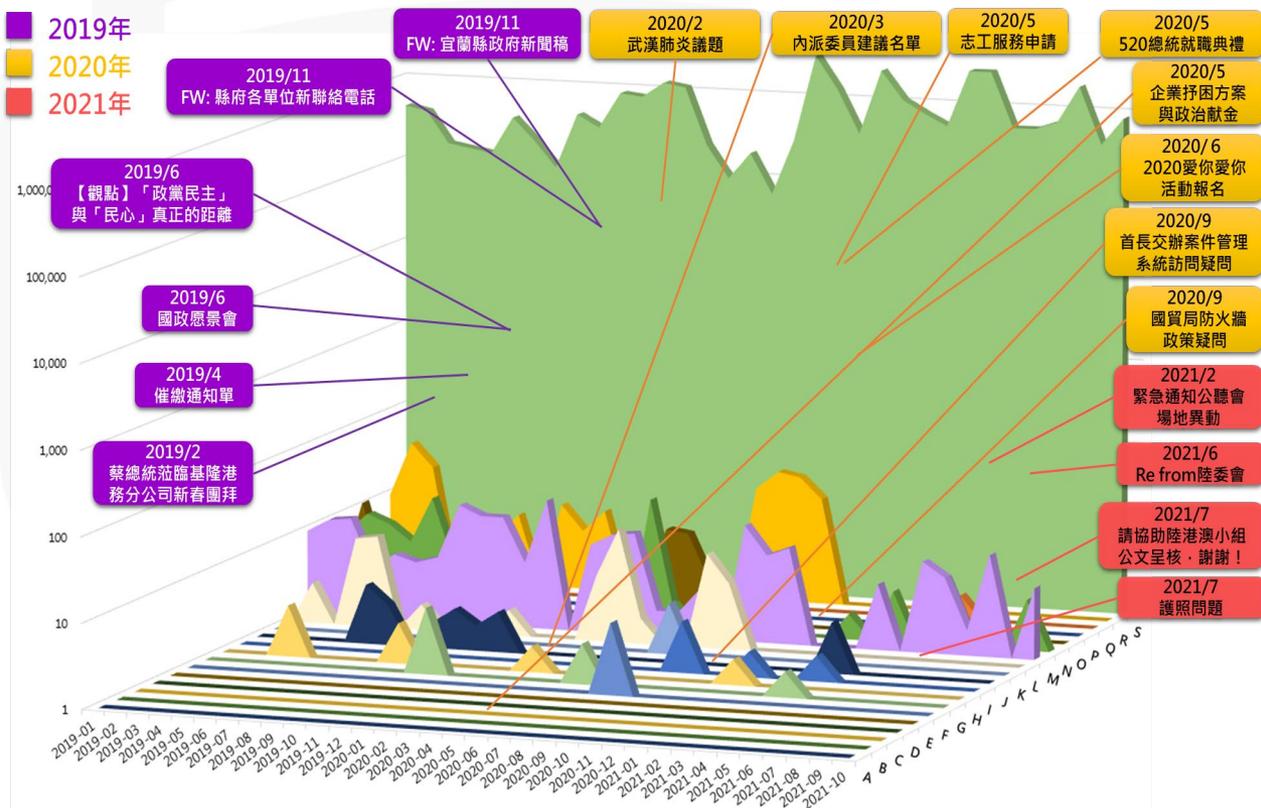
服務公開於網際網路  
可直接存取與竄改



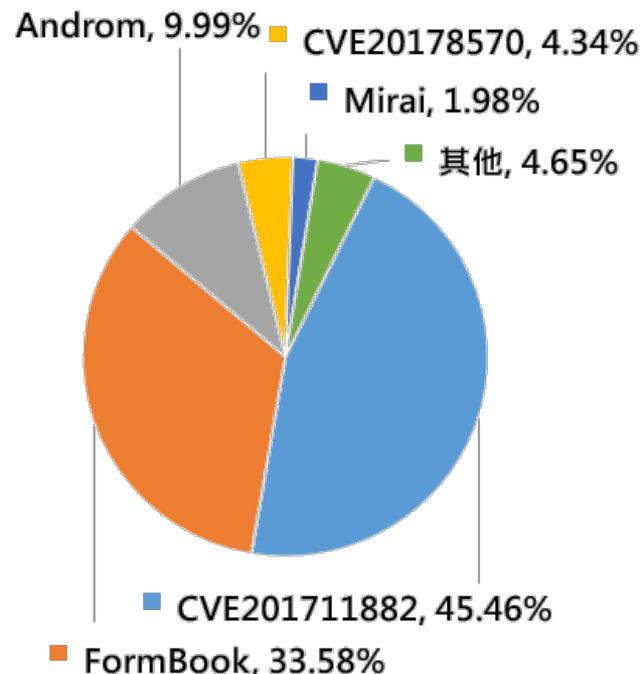
# APT惡意電子郵件攻擊(1/2)

- 電子郵件附檔惡意程式攻擊以**微軟Office文件系列之遠端執行漏洞(CVE-2017-11882)**最多，占整體**45.4%**

– 該漏洞容易觸發且適用平台廣泛，自106年揭露至今仍是惡意文件附檔攻擊最常利用之漏洞



## TOP5郵件附檔惡意程式



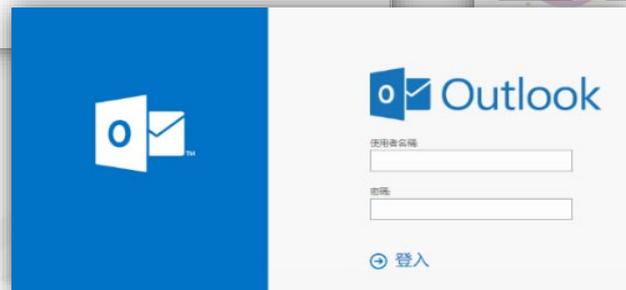
# APT惡意電子郵件攻擊(2/2)

- 110年政府領域APT惡意電子郵件攻擊

- 以請求政府機關業務辦理窗口協助為主旨，進行APT惡意電郵攻擊
- 110年中起發現駭客大量註冊與政府機關相似網域，並偽冒機關常見網頁郵件(Webmail)登入頁面，發動社交工程釣魚郵件攻擊

- 駭客將中繼站偽裝為正常機關網站混淆使用者

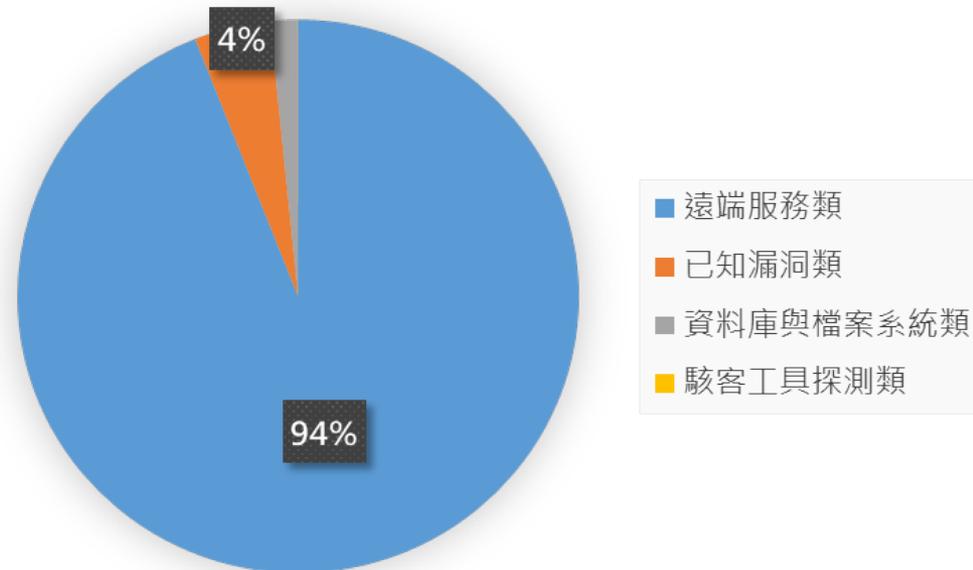
- E-GOV(域名：[api.gov-tw.workers.dev](http://api.gov-tw.workers.dev))、FTC(域名：[mergers.ftclibrary-gov.com](http://mergers.ftclibrary-gov.com)、[mergers.ftc-gov.workers.dev](http://mergers.ftc-gov.workers.dev))



# 遠端服務探測與產品漏洞威脅

- 110年1~10月政府骨幹網路主要威脅類型為遠端服務探測，包含RDP遠端桌面連線
- 以**網通設備**與**VPN設備**漏洞為主，包含微軟 Exchange Server、Vmware及Citrix商業產品漏洞

駭客針對機關網路設備與對外服務進行漏洞探測



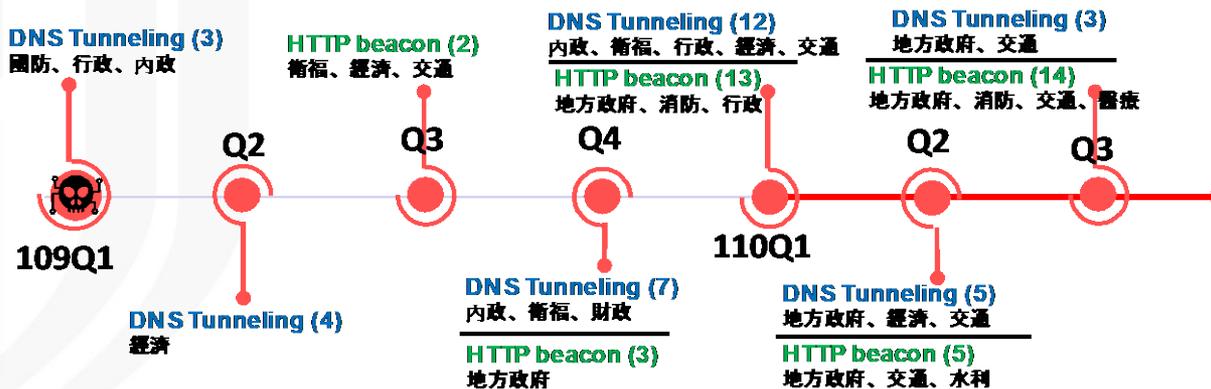
# Cobalt Strike後門回報行為盛行



- 109年起陸續發現政府機關遭到入侵，主要透過DNS Tunneling通道與HTTP Beacon進行資料竊取與命令控制
- Cobalt Strike為用於紅隊演練之滲透測試軟體，被發現用來進行APT攻擊<sup>[1]</sup>，如APT19、APT32、**APT41**<sup>[2]</sup>、Cobalt Group及**Chimera**<sup>[3]</sup>等



機關受駭事件較  
往年增加100%



資料來源：

1. <https://attack.mitre.org/software/S0154/>
2. <https://www.inside.com.tw/article/20988-5-china-apt-41-hackers-have-aggressively-attacked-taiwan>
3. <https://www.cw.com.tw/article/5102090>

- 資通安全威脅趨勢與案例分享
  - 全球資通安全威脅趨勢
  - 政府資通安全威脅趨勢
  - 政府資安事件案例分享
- 政府機關資安防護強化重點
  - 落實資安縱深防禦
  - 善用通報應變網站情資分享
- 結論與建議

# 工控與物聯網應用風險案例(1/2)



- 政府機關導入AIoT建置AI智慧路口實驗場域，因未做好MQTT服務保護，衍生下列風險
  - 可啟動特定路口號誌，進行動態調整
  - 可更改監測資訊，影響號誌監測機制
  - 號誌監測系統暴露，存在阻斷服務風險
- 水利單位之水利設備工控人機管理介面(HMI)，可使用預設帳號密碼存取並進行控制

設備人機管理介面(HMI) 暴露於網路，並使用預設帳密



No.	觸發時間	描述	數值	邏輯	End Time
100	2021/06/25 01:35:41	沉水架M1-啟停命令	ON	Auto	---
99	2021/06/24 17:44:59	沉水架M1-啟停命令	ON	Manual	---
98	2021/06/07 23:03:37	沉水架M2-啟停命令	ON	Auto	2021/08/07 23:04:36
97	2021/06/07 23:01:24	沉水架M2-啟停命令	ON	Auto	2021/08/07 23:01:44
96	2021/06/07 22:53:06	沉水架M2-啟停命令	ON	Auto	2021/08/07 22:56:27
95	2021/06/07 22:52:44	沉水架M1-啟停命令	ON	Auto	2021/08/07 22:53:05
94	2021/06/07 22:51:47	沉水架M2-啟停命令	ON	Auto	2021/08/07 22:52:34
93	2021/06/07 22:50:18	沉水架M1-啟停命令	ON	Auto	2021/08/07 22:51:47
92	2021/06/07 22:45:19	沉水架M1-啟停命令	ON	Auto	2021/08/07 22:46:11
91	2021/06/07 22:41:31	沉水架M1-啟停命令	ON	Auto	2021/08/07 22:43:40
90	2021/06/07 18:55:07	沉水架M1-啟停命令	ON	Manual	---
89	2021/08/06 10:47:54	沉水架M1-啟停命令	ON	Manual	2021/08/06 10:48:11
88	2021/08/06 08:05:22	沉水架M2-啟停命令	ON	Manual	2021/08/06 10:48:11
87	2021/08/06 02:09:00	沉水架M2-啟停命令	ON	Auto	2021/08/06 02:01:00
86	2021/08/05 07:12:56	沉水架M2-啟停命令	ON	Manual	2021/08/06 10:48:11
85	2021/08/05 02:00:00	沉水架M1-啟停命令	ON	Auto	2021/08/05 02:01:00
84	2021/08/04 26:29:27	沉水架M2-啟停命令	ON	Manual	2021/08/04 20:30:06

路口號誌啟動動態號誌 可遭到調整

```
TRAFFIC/CONTROL/5
{
  'RoadID': '5', 'SwitchDynamic': True,
  'Datetime': '2021-04-26 11:15:02'
}
```

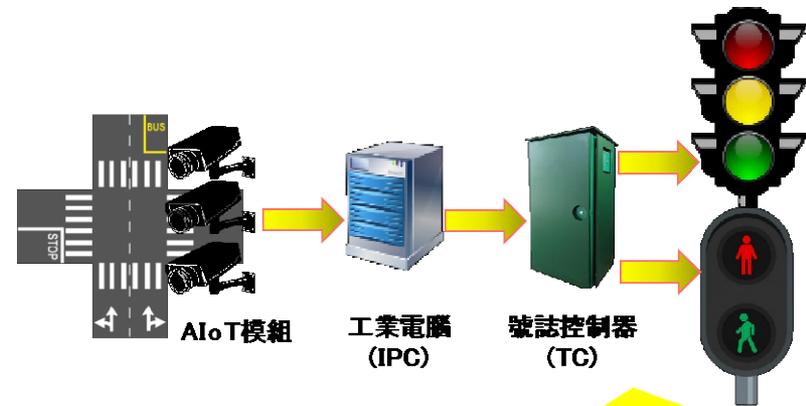
# 工控與物聯網應用風險案例(2/2)



## 防護建議

- 規劃AIoT與工控系統聯網時，應盤點相關IT與OT資產並納入風險評估
- 物聯網外點設備存取導入VPN機制
- 人機管理介面(HMI)應進行帳號密碼強化與連線管理

No.	觸發時間	觸發	數值	種類	End Time
100	2021/08/25 01:35:41	汎水廠M1-啟停命令	ON	Auto	---
99	2021/08/24 17:44:39	汎水廠M1-啟停命令	ON	Manual	---
98	2021/08/07 23:03:17	汎水廠M1-啟停命令	ON	Auto	2021/08/07 23:04:36
97	2021/08/07 23:01:24	汎水廠M1-啟停命令	ON	Auto	2021/08/07 23:01:44
96	2021/08/07 22:53:06	汎水廠M1-啟停命令	ON	Auto	2021/08/07 22:56:27
95	2021/08/07 22:52:34	汎水廠M1-啟停命令	ON	Auto	2021/08/07 22:53:05
94	2021/08/07 22:51:47	汎水廠M1-啟停命令	ON	Auto	2021/08/07 22:52:34
93	2021/08/07 22:50:18	汎水廠M1-啟停命令	ON	Auto	2021/08/07 22:51:47
92	2021/08/07 22:49:19	汎水廠M1-啟停命令	ON	Auto	2021/08/07 22:46:11
91	2021/08/07 22:41:31	汎水廠M1-啟停命令	ON	Auto	2021/08/07 22:43:46
90	2021/08/07 09:53:37	汎水廠M1-啟停命令	ON	Manual	---
89	2021/08/05 18:47:54	汎水廠M1-啟停命令	ON	Manual	2021/08/05 18:48:11
88	2021/08/05 09:05:22	汎水廠M1-啟停命令	ON	Manual	2021/08/05 10:48:11
87	2021/08/05 02:03:00	汎水廠M1-啟停命令	ON	Auto	2021/08/05 02:01:06
86	2021/08/05 07:12:56	汎水廠M1-啟停命令	ON	Manual	2021/08/05 10:48:11
85	2021/08/05 02:00:00	汎水廠M1-啟停命令	ON	Auto	2021/08/05 02:01:06
84	2021/08/04 26:29:27	汎水廠M1-啟停命令	ON	Manual	2021/08/04 20:30:06



針對SCADA HMI管理設備與介面，  
納入資產盤點並進行存取管理

外點設備之存取與管理，應納入管制  
例如：行動網路VPN(Mobile Data  
Virtual Private Network, MDVPN)

# 電子郵件帳密遭暴力破解攻擊

- 110年發現多個機關電子郵件帳號遭到利用，寄送社交工程釣魚郵件與惡意程式垃圾郵件
- 多為無限制外部存取與提供網頁登入之郵件伺服器



## 防護建議

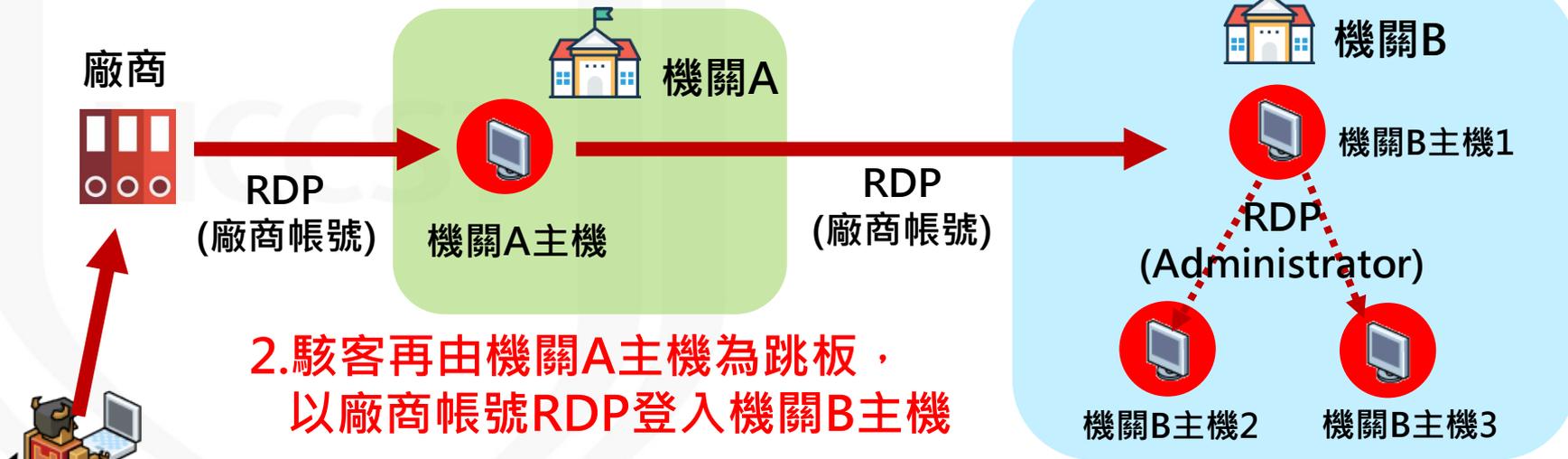
- 應強化電子郵件帳號密碼強度及定期更改密碼
- 應加強郵件伺服器錯誤登入嘗試次數設定

# 供應鏈/委外廠商管理案例(1/2)



- 駭客藉由委外廠商合法管道，使用RDP服務入侵機關A主機，並以機關A主機為跳板入侵機關B
- 在機關B使用相同帳號密碼，進行橫向擴散攻擊

1. 駭客使用廠商IP當跳板，  
以廠商帳號RDP登入機關A主機



2. 駭客再由機關A主機為跳板，  
以廠商帳號RDP登入機關B主機

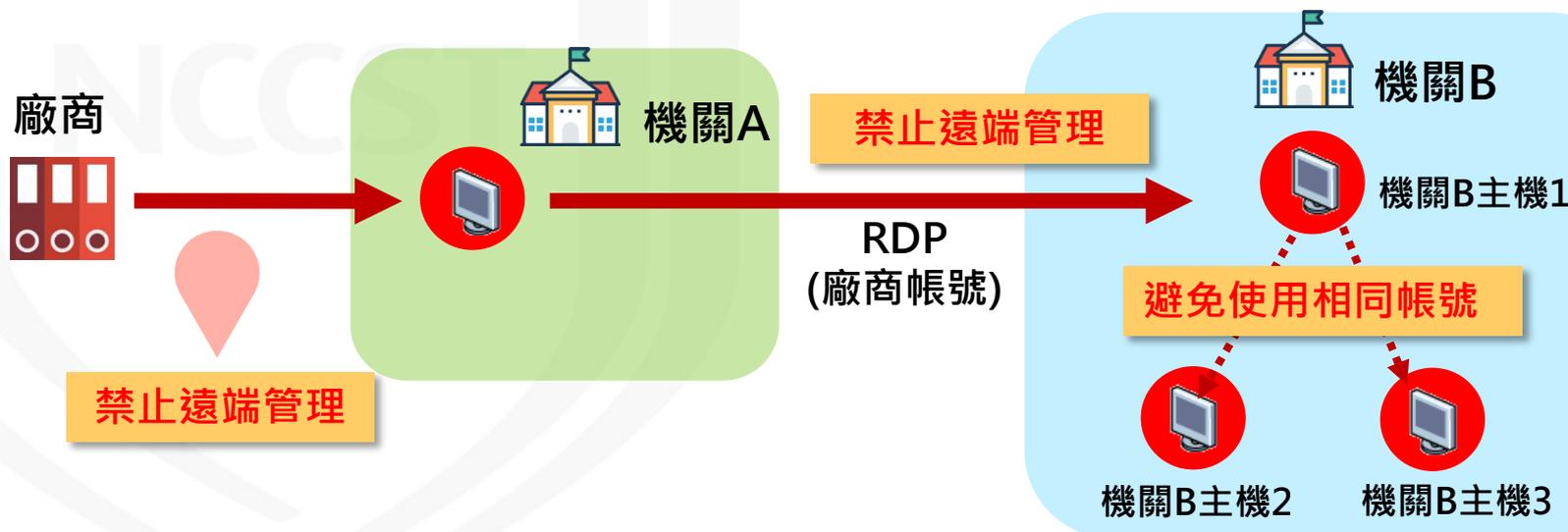
3. 機關B內網主機使用相同帳密，  
遭駭客進行內部擴散

# 供應鏈/委外廠商管理案例(2/2)



## 防護建議

- 機關應禁止開放廠商遠端管理，並避免使用相同之本機帳號密碼
- 導入多因子驗證(Multiple Factor Authentication, MFA)，限制使用者以管理員帳號登入本機電腦
  - ✓ 停用/修改Administrator帳號名稱



# 資訊集中機房橫向擴散案例(1/3)



- CobaltStrike工具使用HTTP(S)或DNS隧道通訊(DNS Tunnel)等加密技術，躲避偵測/阻擋機制，部分防護設備與資安服務廠商無法有效防範



- 偽裝成正常Web流量以規避流量檢測
- 租賃雲端服務增加混淆，傳統IP連線分析/阻擋機制失效

```
GET /jquery-3.3.1.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Referer: http://code.jquery.com/
Accept-Encoding: gzip, deflate
Cookie: __cfduid=CQ5subE05f9AV0zNgW2c
RXbIC3qHkG6sE_QjxZ-
X_X5STlgA5YceQOEChVC8s6MX6GBziFEWxw
cFPDu32WqNcsc
User-Agent: Mozilla/5.0 (Windows NT
Host: 10.3.97.106
Connection: Keep-Alive
Cache-Control: no-cache
```

偽冒正常jQuery  
網頁瀏覽

- 將訊息偽裝成大量隨機域名查詢
- 受害主機與控制主機無直接連線，傳統IP連線分析/阻擋機制失效

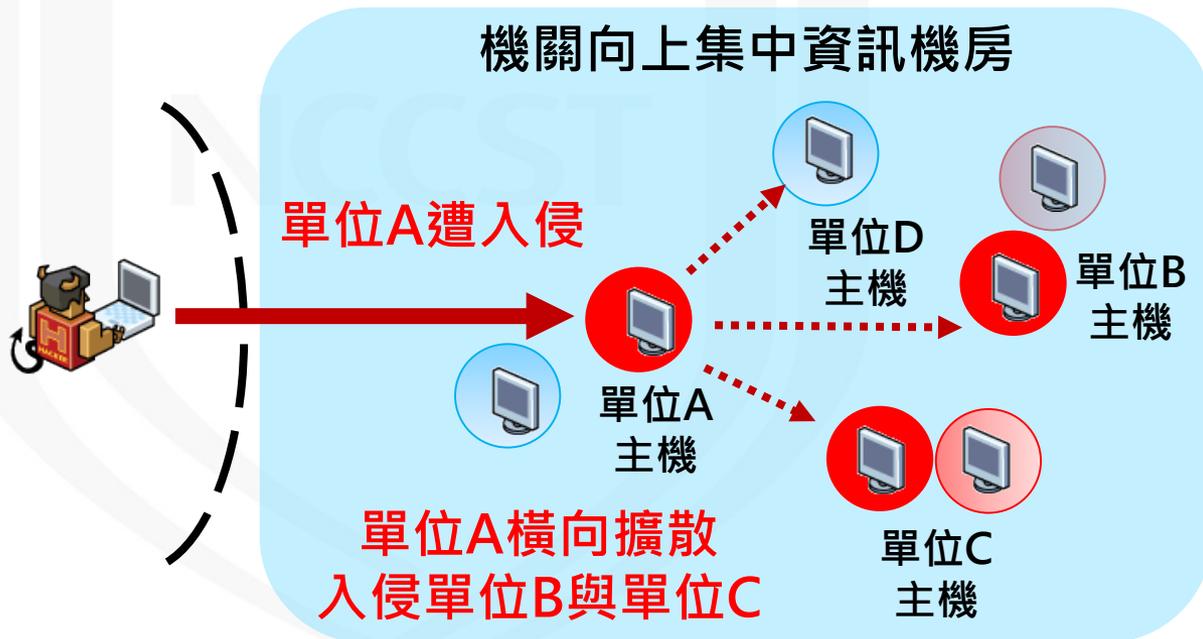
```
woqs67.287ab4237acfeb53ae28b145713a1fc8af6b7fd8e49c6882f752b031d.cdb1bc5dd45c22e885b5f1b770ed4a3c0e
7xe4q.180.064e006b8.35c274be.ns.microsoftdown.dnsrd.com
7xe4q.196bca4a2.364e006b8.35c274be.ns.microsoftdown.dnsrd.com
1zc.0bc5634a.35c274be.ns.microsoftdown.dnsrd.com
7xe4q.180.0756a4ef0.35c274be.ns.microsoftdown.dnsrd.com
7xe4q.36f45023d92542a2.35c274be.ns.microsoftdown.dnsrd.com
7xe4q.196bca4a2.3756a4ef0.35c274be.ns.microsoftdown.dnsrd.com
1zc.044da0519.35c274be.ns.microsoftdown.dnsrd.com
```

偽裝並產生大量域名查詢  
{xx 亂數}.ns1.mal.com

# 資訊集中機房橫向擴散案例(2/3)



- 機關向上集中架構之資訊機房，所屬單位A收到下載CobaltStrike工具警訊，機關僅針對單位A進行處理
- 駭客從外網入侵後，以RDP暴力破解方式進行橫向擴散，入侵單位B與單位C
- 單位B進行事件調查，發現橫向擴散事件



- 機關向上集中機房未部署端點防護與內網偵測機制
- 受駭後忽略CoblaStrike入侵樣態，未全面進行擴散調查

# 資訊集中機房橫向擴散案例(3/3)



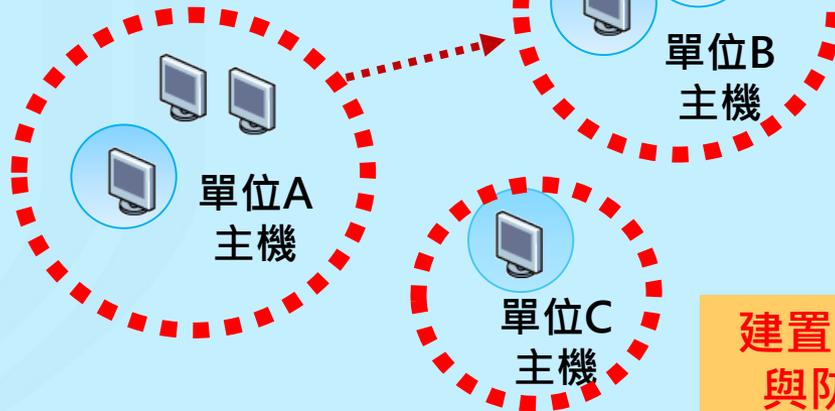
## 防護建議

- 針對向上集中資訊機房，可針對不同單位(用途)規劃不同子網段，並採白名單連線管理
- 建議於資訊向上集中架構中，建置偵測與防護機制(如端點防護與IPS等)



### 機關向上集中資訊機房

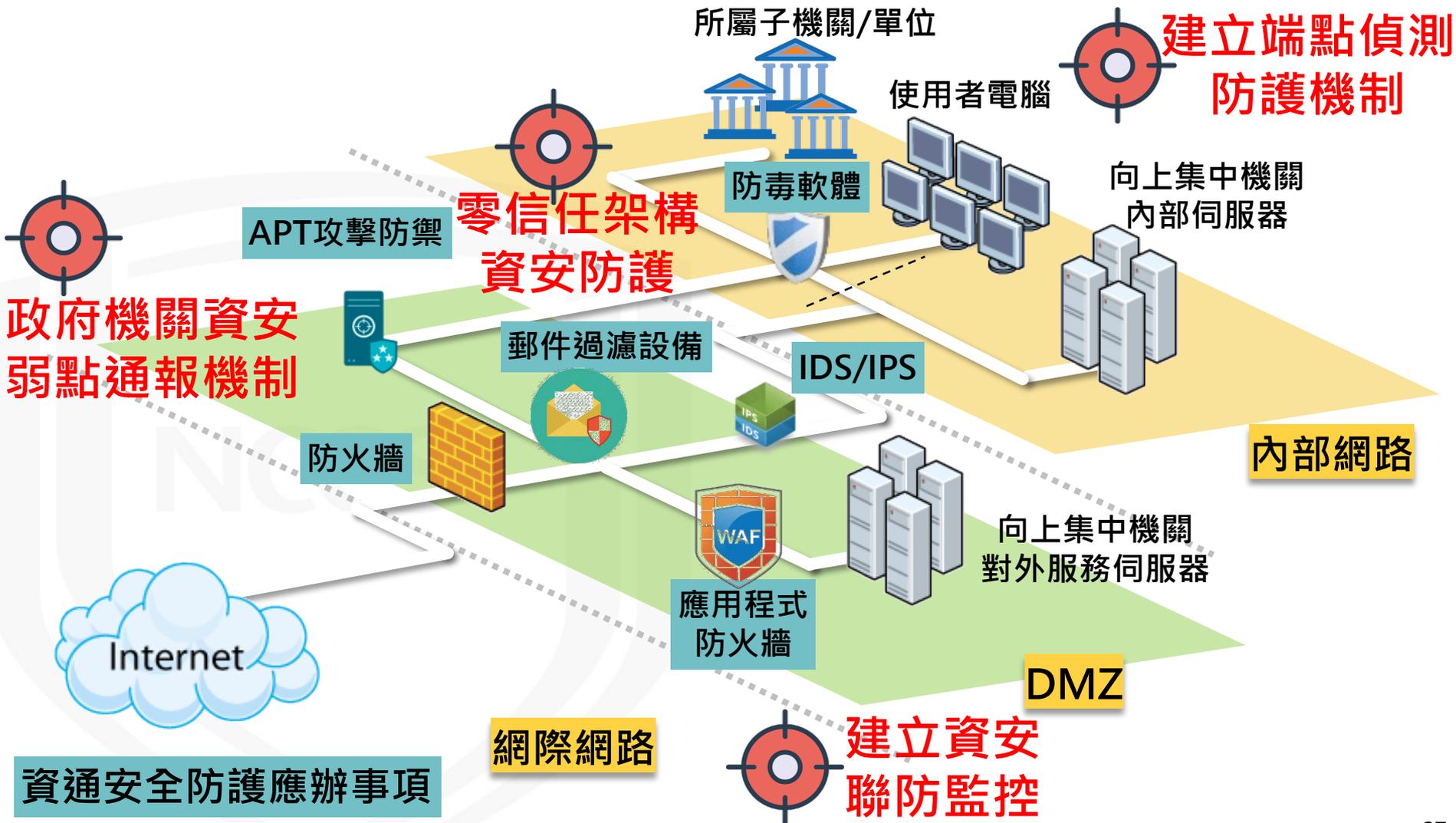
區分各單位子網段



建置威脅偵測  
與防護機制

- 資通安全威脅趨勢與案例分享
  - 全球資通安全威脅趨勢
  - 政府資通安全威脅趨勢
  - 政府資安事件案例分享
- 政府機關資安防護強化重點
  - 落實資安縱深防禦
  - 善用通報應變網站情資分享
- 結論與建議

# 落實資安縱深防禦



# 導入政府機關弱點通報機制

- 機關應配合資通安全管理法要求，導入政府機關資安弱點通報機制(Vulnerability Alert and Notification System, VANS)
  - 盤點資通系統並標示核心資通系統與相關資產
  - 建立風險評估機制，針對盤點資產進行資安風險評估

## VANS系統

### 資產管理



- 系統化管理資訊資產
- 下載軟體資產CPE清單

### 弱點管理



- 接收弱點通知
- 掌握安全性更新落實程度

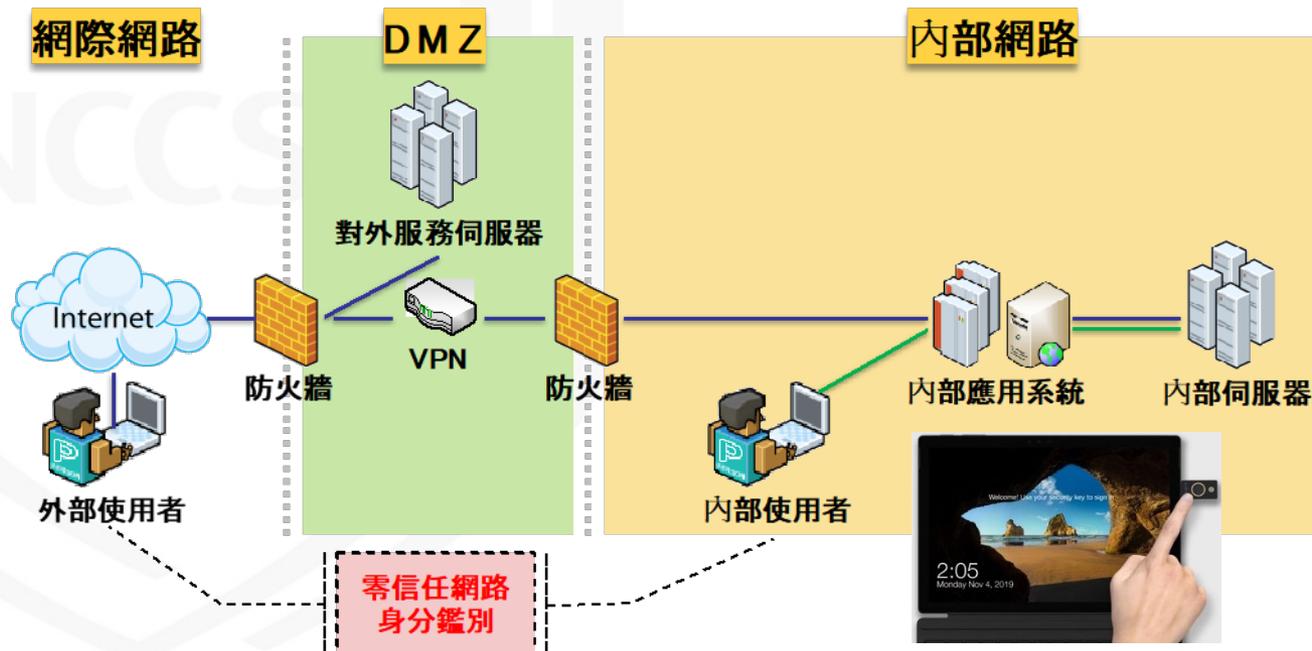
### 資訊綜整



- 即時掌握機關弱點分布情形
- 掌握資訊資產受影響狀況

# 導入零信任架構

- 機關於內外網導入零信任網路身分鑑別機制
- 使用多因子驗證(Multiple Factor Authentication, MFA)強化資安防護能力
  - 例如：使用符合FIDO2規範之硬體密碼鑑別器，進行雙因子無密碼登入



# 落實資安監控與防護(1/3)

- 經政府資安監控有效性驗證，針對資安事件通報統計，機關回報未納入監控範圍比例略高，顯見監控範圍急需檢視與改善

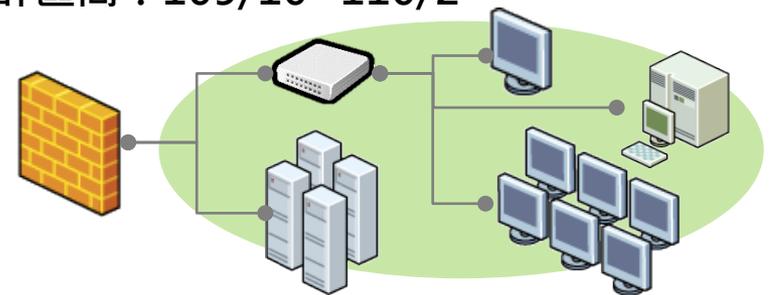
- 網路攻防演練48.1%
- 技服中心資安警訊58%
- 機關通報資安事件45%

偵測能力項目	未納入監控範圍比例
網路攻防演練	48.1%(共27則)
技服中心資安警訊	58%(共112則)
機關通報資安事件	45%(共91則)

統計區間：109/10~110/2

- 監控範圍認定

- 資訊資產是否在資通安全防護項目監控範圍內



- 機關應於資安事件結報流程，填寫受駭主機是否納入監控範圍

# 落實資安監控與防護(2/3)



- 機關應針對新興威脅與資安事件，盤點現有資安防護部署與監控能量，確保涵蓋度與有效性

– 如針對DNS日誌收容與分析，挖掘DNS Tunnel異常行為

– 針對資安威脅指標防護，建議採取正確偵測與防護措施

➤ 例如：DNS Tunnel無法以阻擋惡意域名方式進行阻擋

➤ 完整域名(FQDN)建議以DNS黑名單與IPS機制避免影響正常服務



## HTTP(S) Beacon 威脅指標



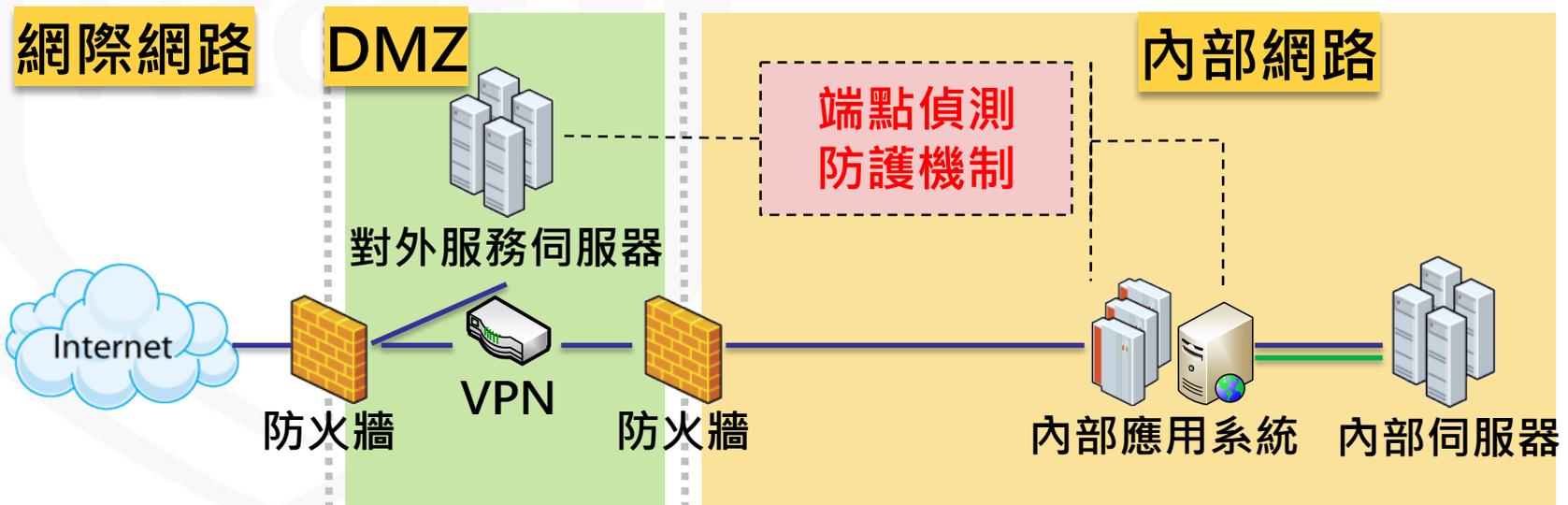
## DNS Tunnel 威脅指標

- 域名型態指標，建以IPS與DNS防護機制，勿使用傳統型態行為
- (X)防火牆設備解析域名對應IP後進行阻擋，影響正常服務
- 雲端平台服務(AWS Cloudfalre、Azure與Google Cloud)
- 中繼站暫時設定為正常服務IP

- DNS tunnel防護須針對所有域名進行阻擋
- (X)以完整域名(FQDN)進行阻擋，無法有效阻擋大量隨機域名\*.mal.com
- 可使用DNS RPZ(Response Policy Zone)

# 落實資安監控與防護(3/3)

- 端點偵測及應變機制(Endpoint Detection and Response, EDR)之建置與資料回傳，已納入資通安全責任等級A、B級公務機關應辦事項要求
- EDR納入監控範圍，並搭配資訊資產與端點偵測進行關聯分析，注意內網橫向擴散情形
  - 針對所有受駭標的進行處置，避免造成更嚴重的資安事件



# 大綱

- 資通安全威脅趨勢與案例分享
  - 全球資通安全威脅趨勢
  - 政府資通安全威脅趨勢
  - 政府資安事件案例分享
- 政府機關資安防護強化重點
  - 落實資安縱深防禦
  - 善用通報應變網站情資分享
- 結論與建議

# 善用通報應變網站情資分享(1/2)



## ● 資通安全情資分享辦法 第三條情資分享

- 公務機關應進行情資分享
- 特定非公務機關得進行情資分享

通報應變網站設置情資分享管道，  
提供機關進行情資分享

事件通報作業 | 申請查詢作業 | 所屬機關通報列表 | 警訊資料查詢 | **情資分享作業** | 資安訊息公告 | 帳號管理

首頁 >> 歷史情資通報列表

搜尋項目

情資通報時間 起 2021/06/12 迄 2021/07/12

搜尋欄位 情資單編號 搜尋內容

情資類型 全部

排序欄位 情資通報時間 輸出順序 降幕

一頁筆數: 10 第 1 頁, 共 1 頁, 結果共 10 筆

確定



請填寫情資相關資料

◎ 情資相關基本資料

\* \* 為必填項目

*機關(機關名稱)	技服用機關1
*機關OID	NCCST
*通報人	劉
*電話	( 02 ) 27339922
*E-mail	@nccst.nat.gov.tw
*情資內容對象為機關本身	<input type="radio"/> 是 <input type="radio"/> 否, 外部單位名稱
*情資來源 (新聞/報紙/雜誌內容非情資分享範圍)	<input type="radio"/> 內部資安防護機制
	<input type="radio"/> 資安防護設備/軟體
	<input type="radio"/> 資安監控中心 自行建置/委外建置廠商名稱
*情資分析單編號	若無收到分析單, 則填寫無
<input type="radio"/> 其他	

◎ 情資資訊詳情

* 情資類型(點此圖示可下載情資類型說明pdf)	<input type="radio"/> 系統存在共通性弱點 <input type="radio"/> 可疑連線/外部攻擊 <input type="radio"/> 惡意程式 <input type="radio"/> 資訊洩漏 <input type="radio"/> 社交工程郵件 <input type="radio"/> DDOS <input type="radio"/> 其他
*情資說明	請說明本資安情資之發現歷程、各類情資所須資訊及可能造成之損害
*入侵指標(IoC)	惡意程式特徵值 請選擇雜湊演算法 請輸入偵測特徵 新增
*短期應變處置	請說明機關知悉本資安情資後, 強化資安防護之作為或規劃, 若無因應作為則填「無」

可參考說明文件，  
依據情資類型提供  
對應之佐證資料

# 善用通報應變網站情資分享(2/2)



## ● 情資確認與處理

- 尚未送出：機關暫存尚未送出，機關可更新內容或自行刪除
- 待處理：機關成功送資料，尚待技服中心處理，機關可檢視內容或自行刪除
- 已處理：機關提供情資內容完整，可提供技服中心確認
- 未符合情資處理原則：機關提供情資內容有誤或不完整，技服中心無法進一步處理

搜尋項目

情資通報時間 起 2021/06/12 迄 2021/07/12 搜尋欄位 情資單編號 搜尋內容

情資類型 全部 排序欄位 情資通報時間 輸出順序 降冪

進階搜尋功能

一頁筆數: 10 第 1 頁, 共 1 頁, 結果共 10 筆 確定

機關可更新或檢視情資內容 情資單狀態類型

刪除	檢視(更新)	情資通報時間	技服中心處理時間	情資單編號	情資類型	情資說明	處理結果
<input type="checkbox"/>	更新	2021/06/29 17:00:45	尚未填寫		尚未填寫	test	尚未送出
<input type="checkbox"/>	檢視	2021/06/29 16:52:52	尚未填寫	20210629001	社交工程郵件	情資說明	待處理
	檢視	2021/06/22 14:42:38	2021/06/22 15:25:36	20210622003	惡意程式	TEST1 TEST2 TEST3 ...	已處理
	檢視	2021/06/22 11:05:24	2021/06/22 15:26:45	20210622002	系統存在共通性弱點	123	未符合情資處理原則



強化資產盤點與漏洞修補，  
提升弱點防護能力



強化工控與物聯網應用管理，  
降低資安風險



強化資安監控與防護，  
落實資安防禦縱深



提升資安防護意識，  
降低社交工程威脅



落實情資分享與善用聯防情資，  
強化資安聯防綜效



報告完畢  
敬請指教

NCCST