國家資通安全研究院
National Institute of Cyber Security

政府機關資安威脅與防護重點

國家資通安全研究院

大綱

- 資安威脅趨勢與案例分享
- 政府機關資安防護強化重點
- 強化通報資料完整性與正確性
- 結論與建議

資安威脅趨勢與案例分享

- 全球資安威脅趨勢
- 政府資安威脅趨勢
- 政府資安事件案例分享

全球資通安全威脅趨勢

全球資安威脅趨勢

- 參考112年全球資安威脅與相關研究案例，歸納全球資安威脅趨勢

網路釣魚為主要攻擊媒介

隨著人工智慧(AI)與新興技術的出現，112年社交工程攻擊顯著增長，網路釣魚仍是最主要攻擊媒介[1]

物聯網/網通設備漏洞利用

- Cisco IOS-XE零時差攻擊約4萬台設備遭感染[2]
- Gafgyt殭屍網路針對Zyxel路由器漏洞CVE-2017-18368進行數千次攻擊[3]

供應鏈攻擊持續發展中

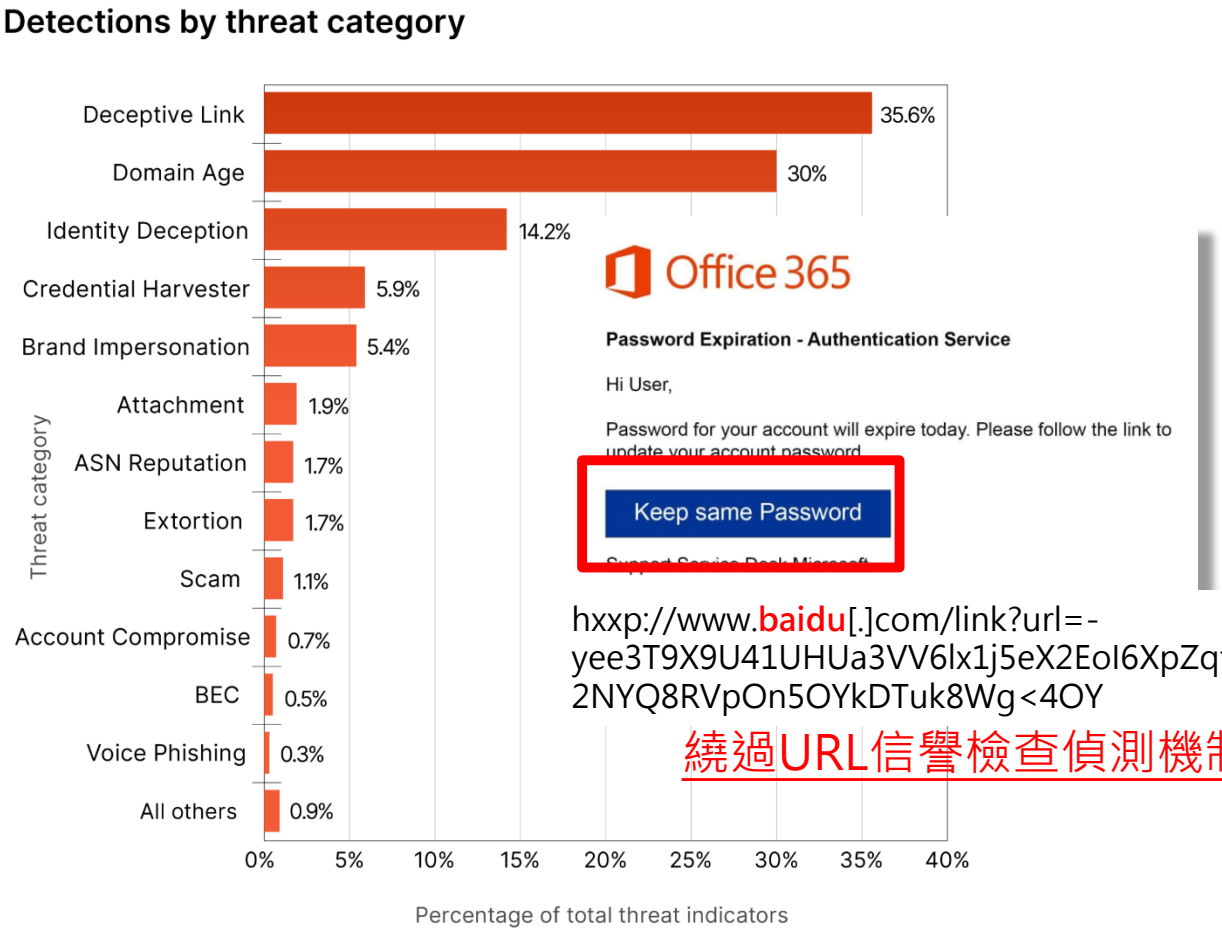
- Gartner預測，114年全球45%組織將遭受軟體供應鏈攻擊[4]
- 112年軟體供應鏈攻擊是108年至111年總和的兩倍[5]

勒索軟體技術多樣化

- 勒索軟體跨Windows、Linux及macOS作業系統進行攻擊[7]
- Veeam指出，93%以上攻擊以備份主機為目標[8]

網路釣魚為主要攻擊媒介

- CISA指出，90%以上網路攻擊都是從網路釣魚開始[8]
  - 冒充受信任的電子郵件或訊息，以詐騙收件人洩漏個人資訊、帳號密碼或執行惡意附件
- 駭客使用欺騙性連結做為網路釣魚策略[9]
  - Cloudflare報告指出，欺騙性連結占網路釣魚威脅35.6%
  - 寄發看似合法URL，使用者點擊該URL可能會導向惡意網站或開啟應用程式(如PDF)，使得駭客可以植入惡意程式或竊取資訊

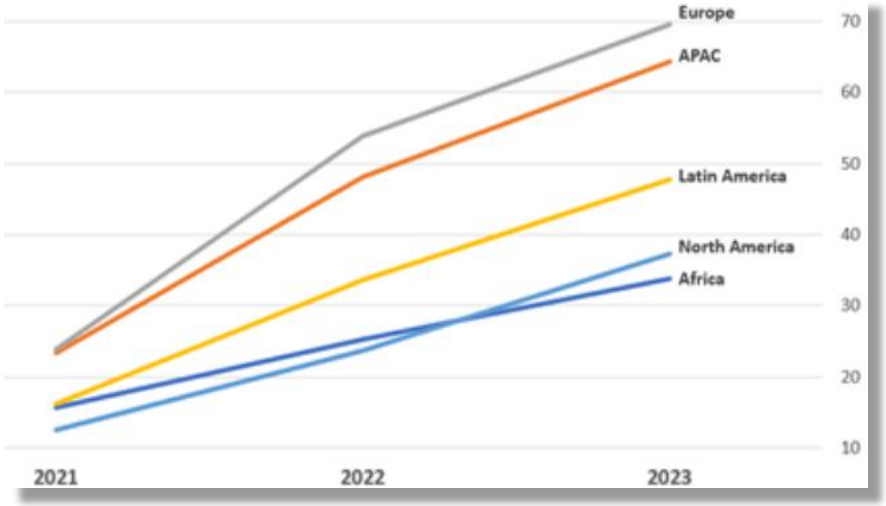


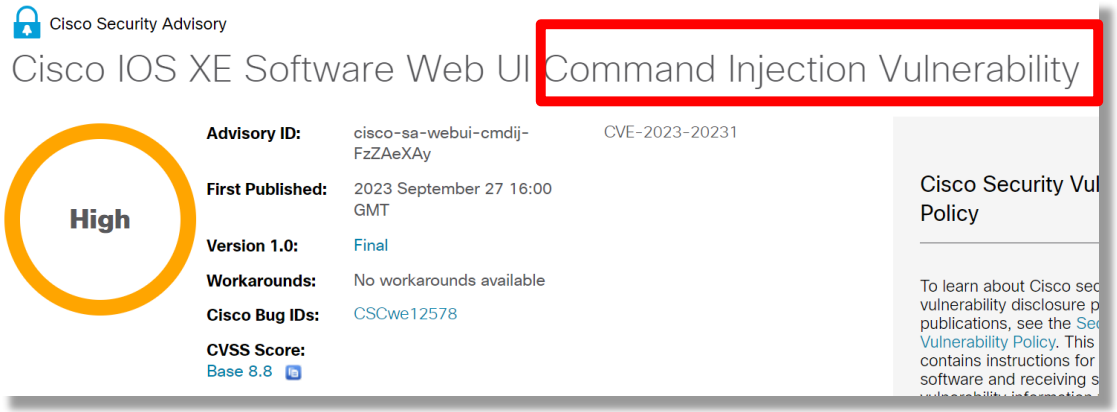
hxxp://www.baidu[.]com/link?url=-yee3T9X9U41UHUa3VV6lx1j5eX2EoI6XpZqfDgDcf-2NYQ8RVpOn5OYkDTuk8Wg<4OY

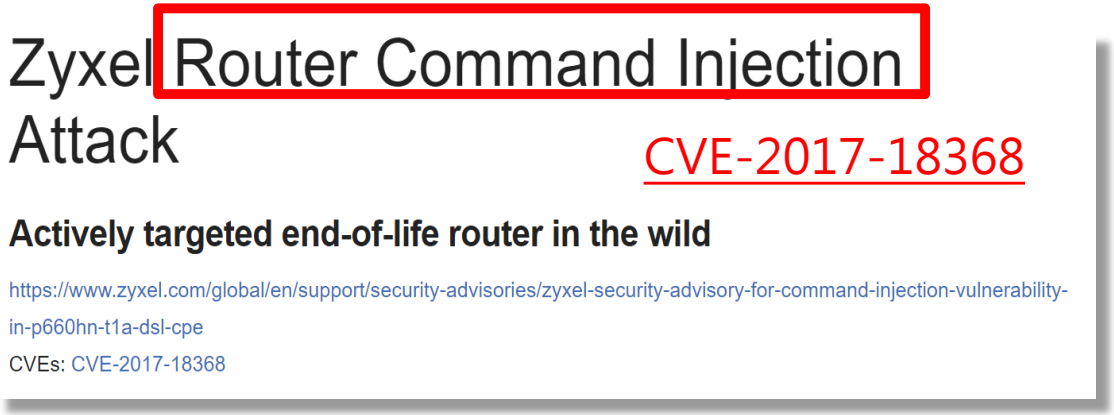
繞過URL信譽檢查偵測機制

物聯網/網通設備漏洞利用

- CheckPoint指出，針對物聯網設備網路攻擊急遽增加[10]
  - 112年與111年相比，物聯網設備平均每週攻擊次數增加41%，平均每週有54%組織遭受攻擊
- 物聯網設備多未有適當的保護或管理，普遍存在注入攻擊[10]
  - 常見受攻擊物聯網設備，如路由器、IP攝影機、DVR(數位錄影機)、NVR(網路錄影機)及印表機等

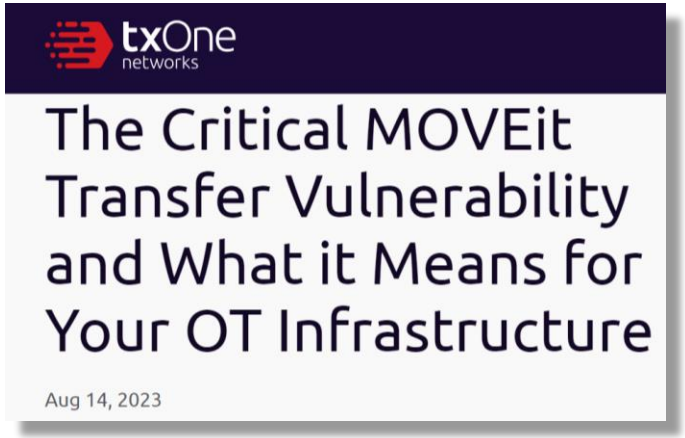






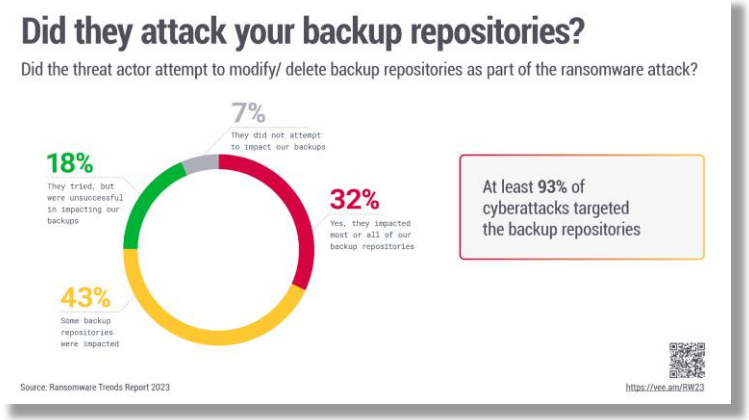
供應鏈攻擊持續發展中

- 供應鏈攻擊係以第三方供應商與服務提供者為目標，以取得對其客戶系統與資料存取權限
  - 零時差/軟體漏洞：針對供應商使用韌體/軟體進行攻擊
  - 憑證竊取：透過網路釣魚或系統漏洞等攻擊取得供應商系統存取憑證
  - 資料竊取：入侵供應商系統取得營運或客戶機敏資料



勒索軟體技術多樣化

- Veeam指出，約93%攻擊以備份檔為目標，近29%無法完成復原
- 造成勒索軟體攻擊主要原因為漏洞利用，其次為憑證洩漏與惡意電子郵件[11]
- 勒索軟體技術多樣化擴及影響平台與規避偵測機制
  - LockBit與Cyclops可感染Windows、Linux及Mac三大作業系統
  - Cactus透過自我加密，繞過防毒軟體偵測機制



AHA warns hospitals about data 'time bombs'

Giles Bruce - Monday, October 2nd, 2023

Save Post Tweet Share Listen Text Size Print Email

Hospitals and health systems should be on the lookout for data "time bombs" that could cause patient information to be destroyed by hackers, the American Hospital Association warned.

Ransomware gangs have been attacking victims twice within close proximity and using data deletion tools that lie dormant during which time the groups can negotiate for more ransom, the FBI said in a notice.

"Cyber adversaries continue to evolve their tactics in a way to increase likelihood of ransom ... said John Riggi, AHA's national advisor for cybersecurity and risk, in a Sept. 29 news

LockBit ransomware encryptors found targeting Mac devices

By Lawrence Abrams — April 16, 2023 — 01:31 PM — 7

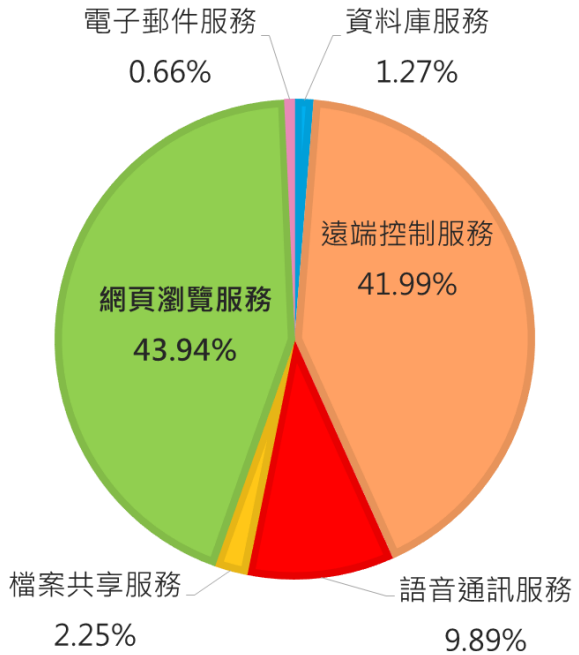
會自我加密的新型勒索軟體 Cactus，讓防毒軟體及網路監控工具偵測不到

作者 Evan | 發布日期 2023 年 05 月 12 日 8:20 | 分類 網路 , 資訊安全 分享 分享 Follow 讚 64 分享

政府資通安全威脅趨勢

殭屍網路威脅情蒐(1/2)

- 112年1月至10月，透過國內外部署之蜜罐誘捕殭屍網路攻擊威脅，共捕獲11,399,806,680次攻擊連線
  - 前3名攻擊跳板來源國家分別為美國(31%)、中國(10%)及新加坡(7%)
  - 針對網頁瀏覽服務之攻擊最為嚴重
  - 捕獲114,054個惡意樣本，以Mirai殭屍網路與其變種最多



殭屍網路威脅情蒐(2/2)

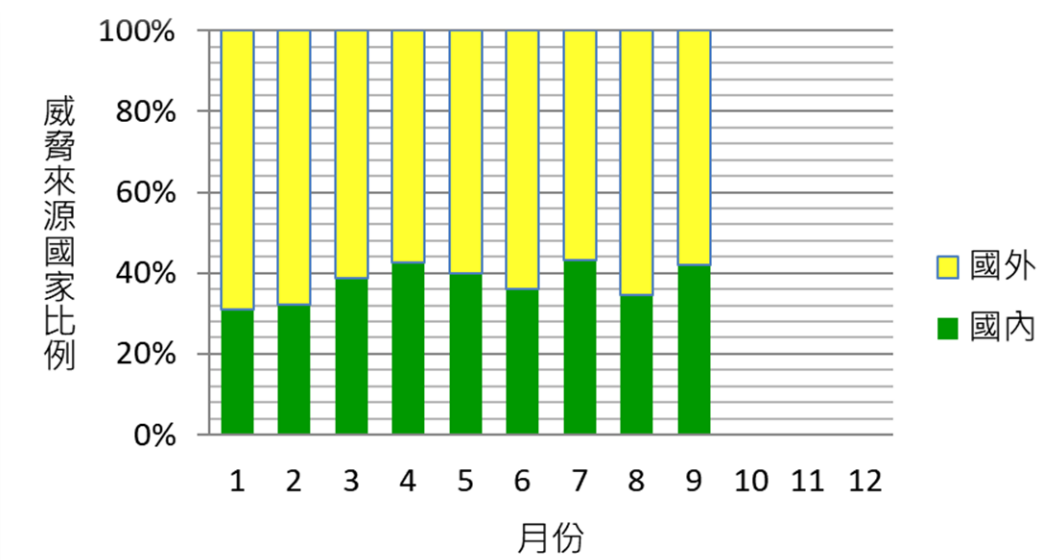
- 112年5月，AndoryuBot出現新型變種，針對物聯網裝置進行感染擴散
  - 不斷利用漏洞持續擴散殭屍網路，並可發起各種協定之DDoS攻擊
  - 駭客集團亦利用此殭屍網路進行營利，於Telegram銷售DDoS攻擊服務
- 駭客建立殭屍網路之動機，可能朝向營利目的之趨勢發展，黑色產業鏈興起，駭客攻擊活動將日益猖獗，升高對我國之資安威脅
  - 需持續宣導物聯網設備之相關威脅風險，提高使用者資安意識，避免設備遭殭屍網路感染

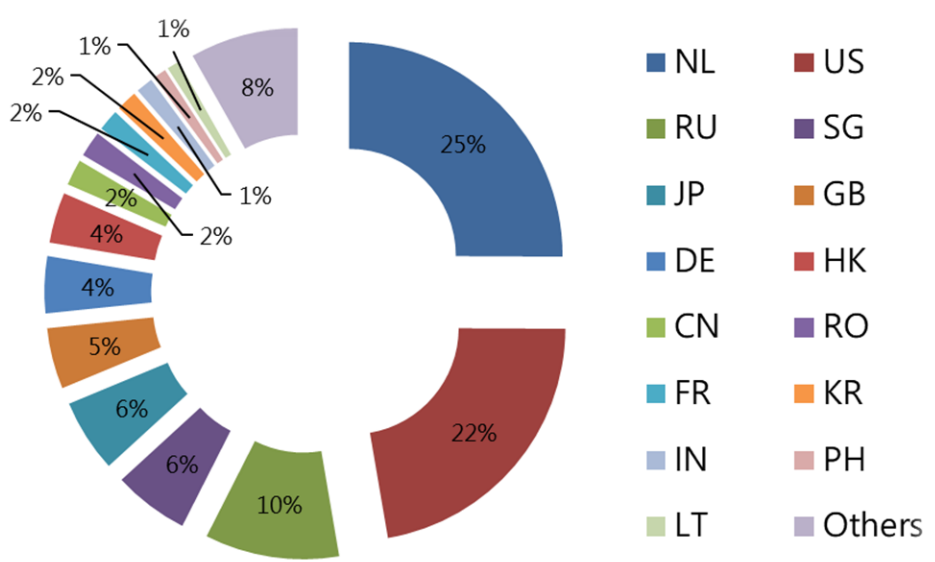
AndoryuBot殭屍網路

- 112年5月，AndoryuBot出現新型變種，以新型漏洞**CVE-2023-25717**進行感染擴散，以Ruckus無線路由器為攻擊目標
- 另2種漏洞之攻擊，以DVR與路由器漏洞注入惡意指令
  - MVPower CCTV DVR之RCE漏洞 (CVE-2016-20016)
  - Dasan GPON路由器之RCE漏洞 (CVE-2018-10562)

聯防監控威脅情蒐(1/2)

- 112年1月至9月，SOC業者回傳有效資安監控情資共516,102件，依政府機關業務類別，前3名分別為外交國防法務類之入侵攻擊68,042件、綜合行政類之資訊蒐集65,658件及外交國防法務類之資訊蒐集61,676件
- 國外攻擊跳板來源前3名分別為荷蘭(25%)、美國(22%)及俄羅斯(10%)





聯防監控威脅情蒐(2/2)

國家資通安全研究院
National Institute of Cyber Security

- 政府領域網通設備為駭客攻擊目標之一

–可程式化邏輯控制器(PLC)暴露影響分析

漏洞編號	CVSSv3分數	漏洞描述
CVE-2022-1161	9.8	屬Rockwell設備遠端程式執行漏洞
CVE-2022-1159	7.2	屬Rockwell設備注入攻擊漏洞
CVE-2022-38773	6.8	屬西門子設備資料完整性驗證漏洞

–機關考勤設備存在零時差漏洞並遭惡意利用

漏洞簡述	漏洞說明
不當的存取控制 (Improper Access Control)	系統存在登入驗證頁面，但未經授權之使用者，可不經身分驗證，存取系統網站頁面。
未限制檔案上傳 (Unrestricted Upload of File)	系統部分頁面存在檔案上傳功能，該功能未過濾特殊字元與驗證檔案類型，未經授權使用者存取該頁面即可上傳任意類型檔案。
危險功能暴露 (Exposed Dangerous Method or Function)	系統部分頁面可直接執行系統指令，未經授權之使用者可存取該頁面，執行任意系統指令。

受攻擊機關類別

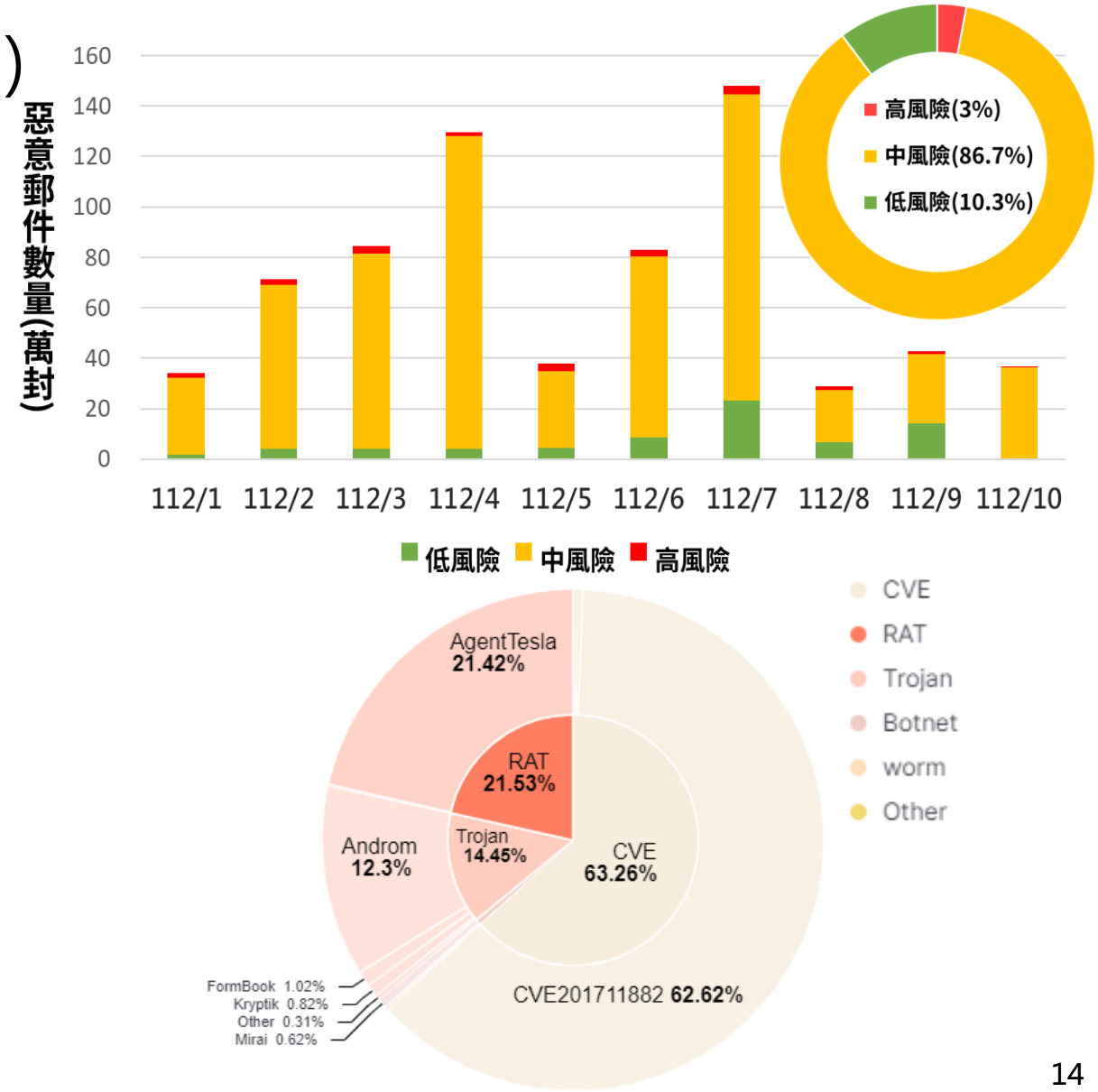
資安責任等級 機關業務類別	B	C	D	總計
綜合行政	3	31	2	36
經濟能源農業	7	0	0	7
總計	10	31	2	43

受攻擊機關類別

資安責任等級 機關業務類別	B	C	D	E	總計
綜合行政	3	2	1	0	6
內政衛福勞動	0	1	17	2	20
教育科學文化	0	3	0	0	3
交通環境資源	0	0	0	2	2
總計	3	6	18	4	31

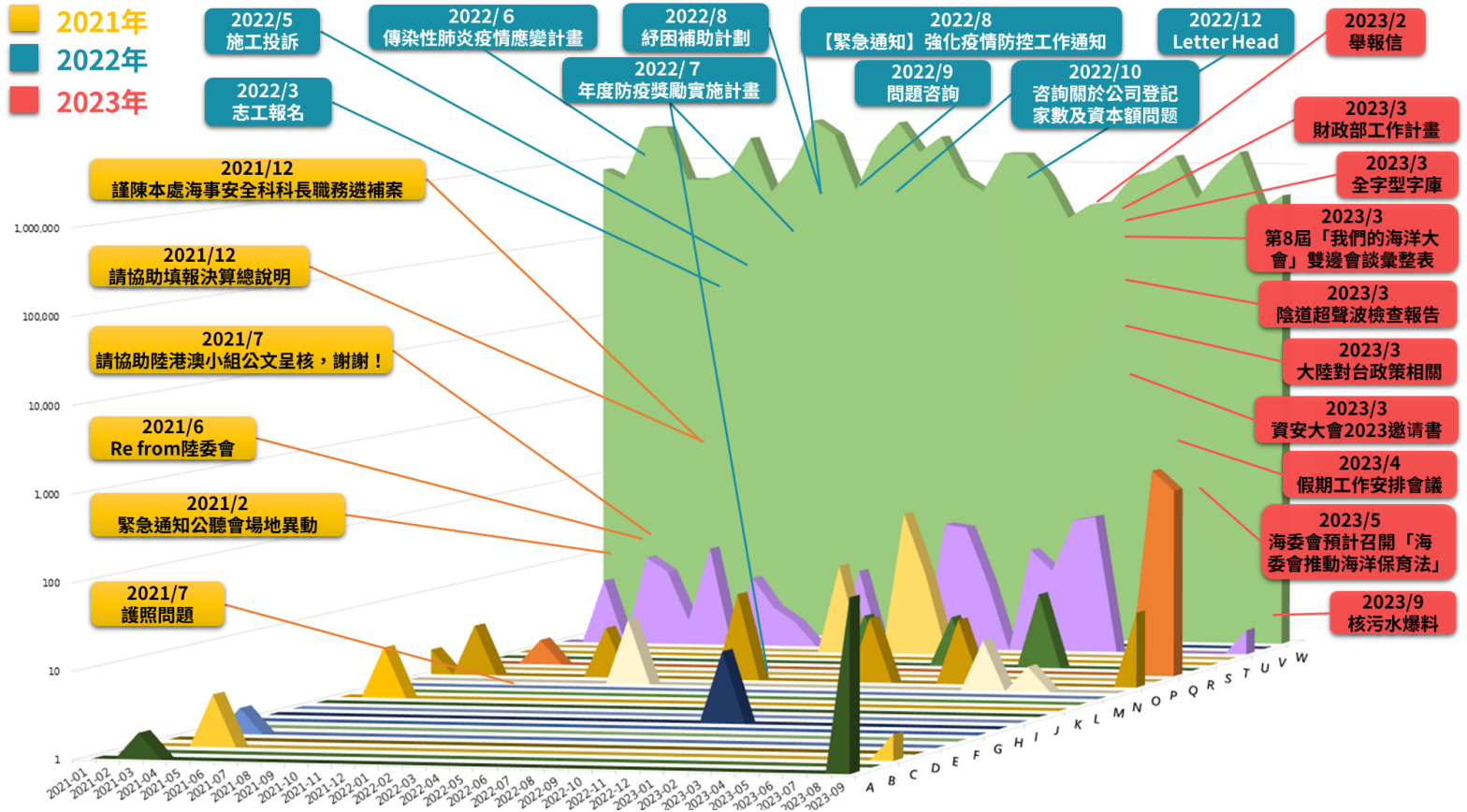
惡意電子郵件分析(1/2)

- 112年共檢測2.8億餘(289,896,041)封電子郵件，偵測發現696萬餘(6,963,081)封可疑惡意電子郵件占2.4%
- 殭屍網路惡意電郵(MalSpam)，以CVE-2017-11882弱點利用攻擊為大宗，占整體惡意程式62.62%，其次偵測之威脅，為AgenTesla遠端木馬與Androm後門木馬等



惡意電子郵件分析(2/2)

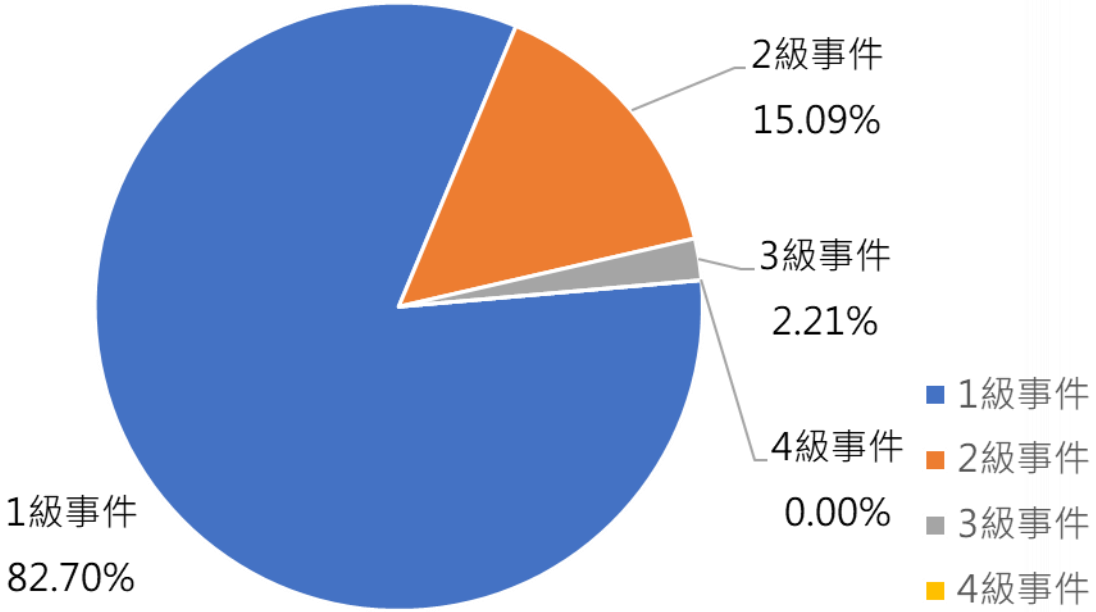
- 112年政府領域APT郵件攻擊趨勢，可歸納為5波攻擊行動，計208封針對性社交工程郵件，其中駭客分別利用政府機關工作業務、會議邀請、健檢報告及檢舉爆料等主旨，對政府機關人員發動攻擊

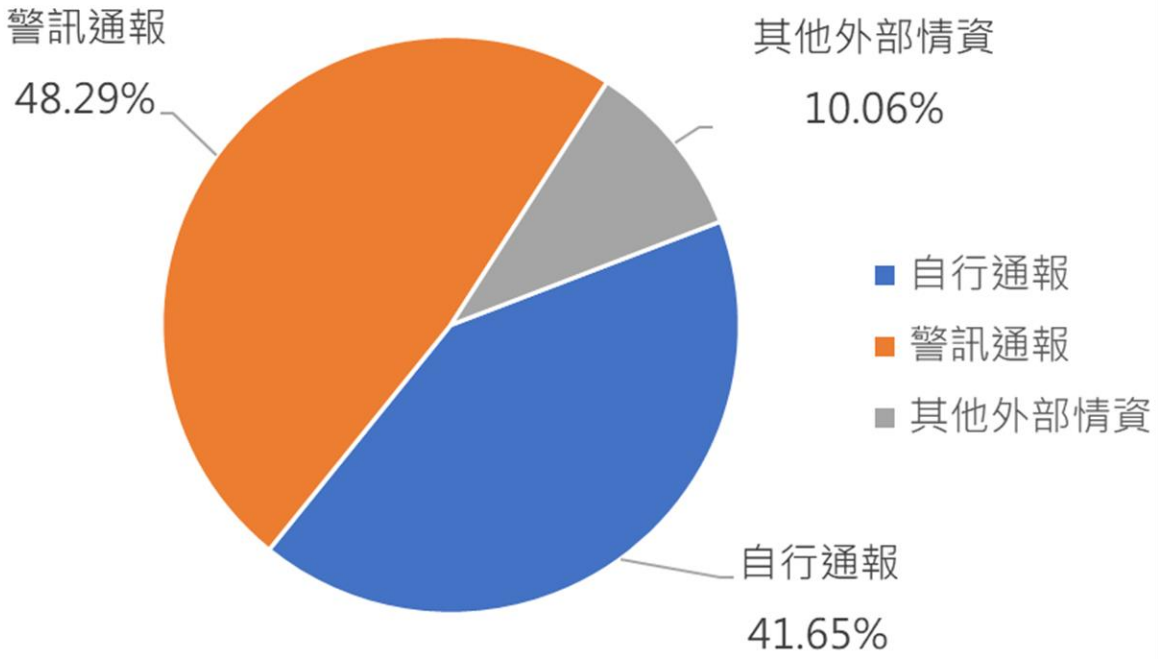


通報事件分析(1/2)

國家資通安全研究院
National Institute of Cyber Security

- 112年1月至9月，共接獲497件政府機關資安事件通報
- 事件影響等級以1級事件為主占82.70%，3級事件僅占2.21%
- 48%為機關接獲資安院警訊通告後所進行之通報



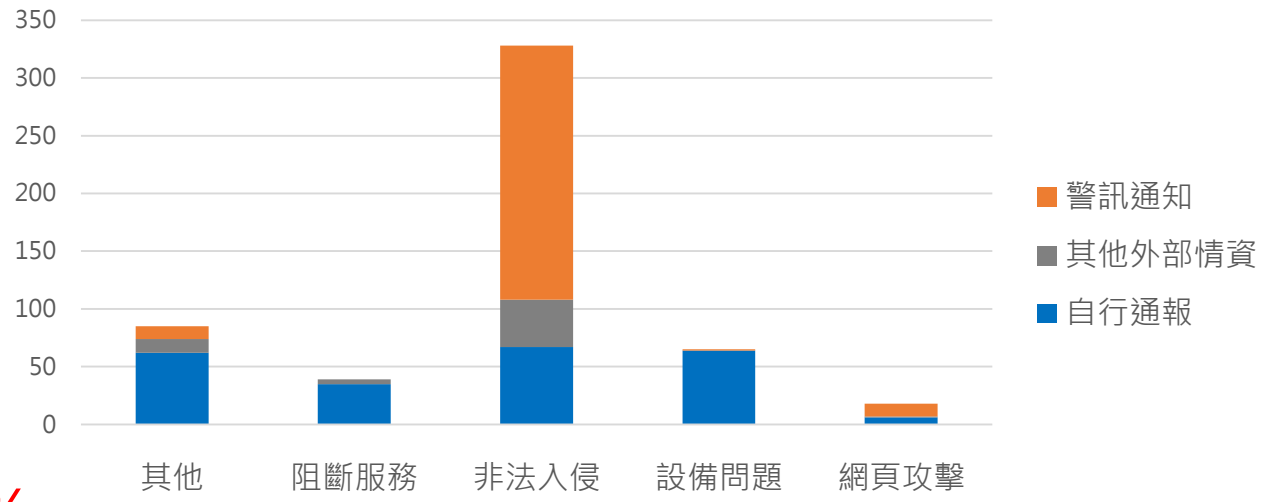


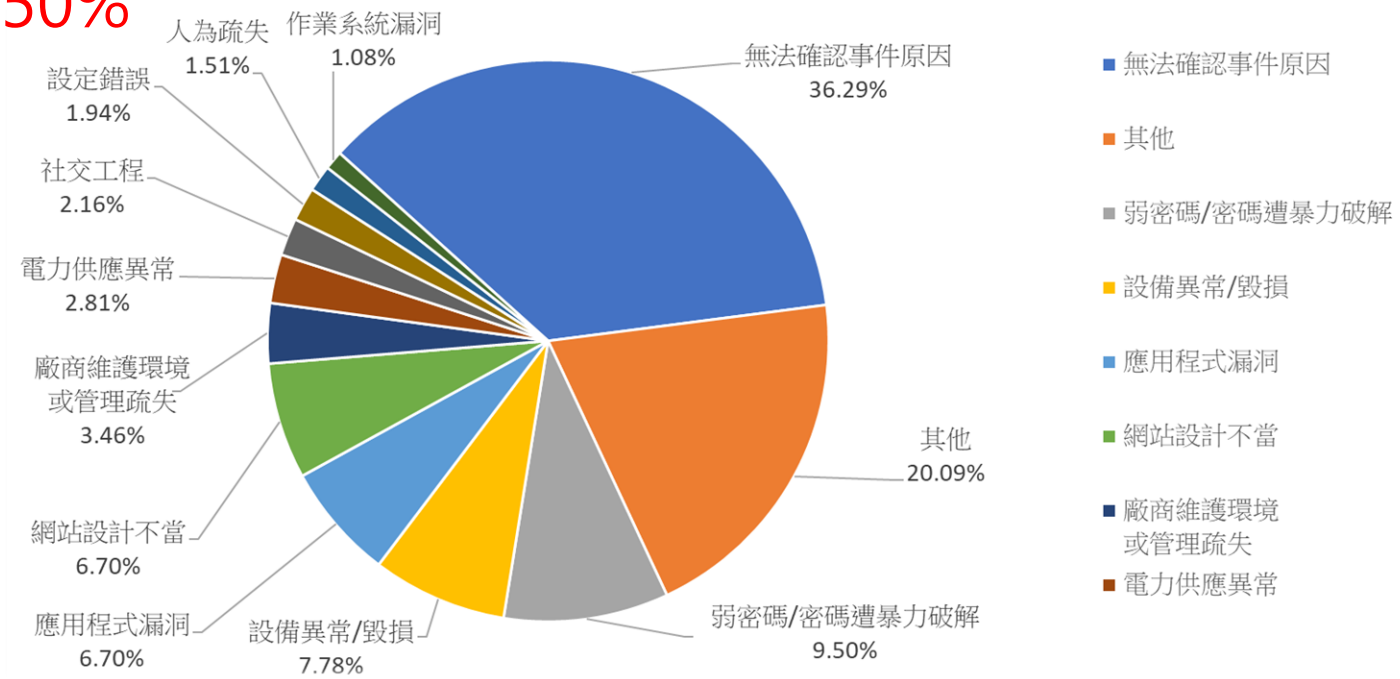
※統計區間：112年1月1日至9月30日

通報事件分析(2/2)

國家資通安全研究院
National Institute of Cyber Security

- 事件類型以非法入侵為大宗，其中又以機關接獲資安院警訊通知後進行通報為主
- 可識別之事件原因
  - 「弱密碼/密碼遭暴力破解」9.50%
  - 「設備異常/毀損」7.87%
  - 「應用程式漏洞」 6.70%





※統計區間：112年1月1日至9月30日

政府資安事件案例分析

近期常見資安事件

案例

人員資安意識不足，開啟惡意郵件，或瀏覽網頁點擊惡意連結

網通設備弱點遭開採利用，增加調查難度

供應鏈廠商遭駭，導致機關出現異常連線

利用產品漏洞發動攻擊，導致帳密外洩

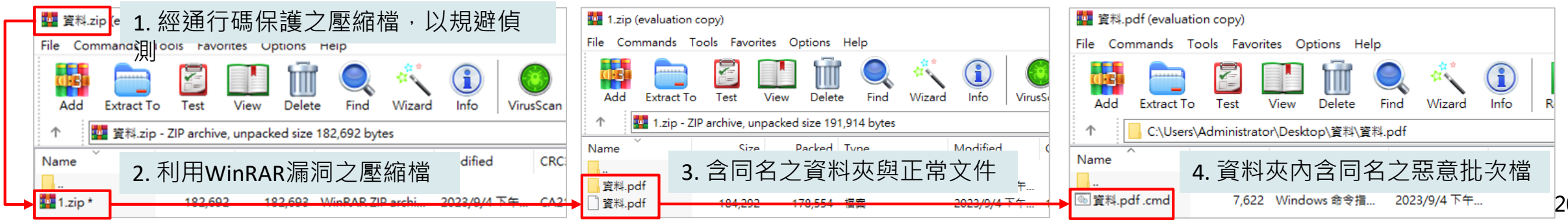
DNS遭DDoS攻擊，無法正常提供服務

漏洞利用社交工程攻擊案例(1/2)

國家資通安全研究院
National Institute of Cyber Security

案情提要

- 駭客利用日本民間公司之郵件帳號，透過VPN服務以核汙水爆料為由，寄送夾帶惡意壓縮檔之社交工程郵件，對政府機關進行社交工程郵件攻擊
- 駭客事先將惡意壓縮檔上傳至匿名文件託管服務，並將下載連結與惡意壓縮檔附於惡意郵件中，壓縮檔則經通行碼保護以規避偵測
- 惡意壓縮檔可觸發近期公告之WinRAR漏洞(CVE-2023-38831)，若使用者點擊誘餌文件，將觸發執行同名資料夾內之惡意批次執行檔
- 經分析，該後門程式為遭駭客濫用之紅隊攻防演練工具Cobalt Strike



漏洞利用社交工程攻擊案例(2/2)

防護建議

- 建議清查與更新WinRAR版本至6.23以上
- 加強內部宣導，注意郵件來源正確性，勿開啟不明來源之郵件與相關附檔及連結

利用WinRAR漏洞製作惡意附檔

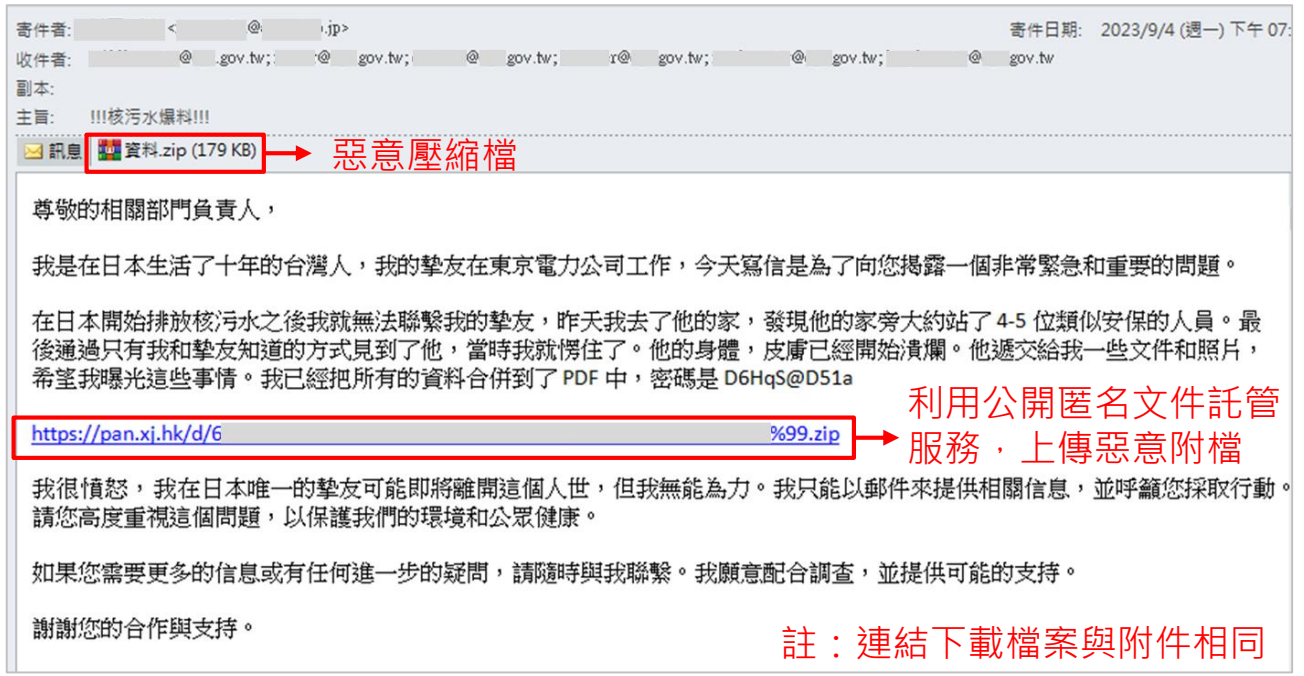
利用VPN服務寄送社交工程郵件

利用匿名文件託管服務上傳惡意檔案

竊取利用日本民間科技公司郵件帳號

核汙水爆料

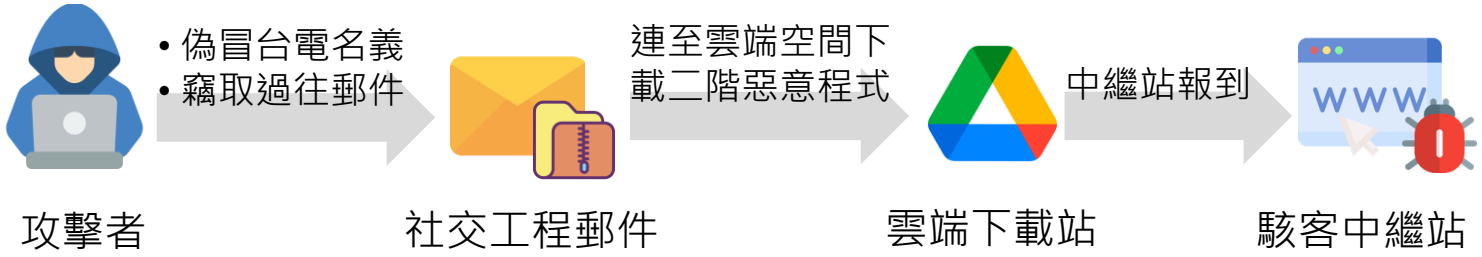
Cobalt Strike



偽冒機關散布惡意電郵案例

案情提要

- 駭客偽冒台電名義與郵件帳號，利用繳交台電費用相關主旨，模仿台電寄送予民眾之繳費通知郵件內文做為誘餌
- 發送以pdf.zip命名之惡意附檔，大量散布惡意程式垃圾郵件，攻擊機關與民眾
- 利用Google雲端空間放置二階NanoCore遠端木馬惡意程式躲避偵測



防護建議

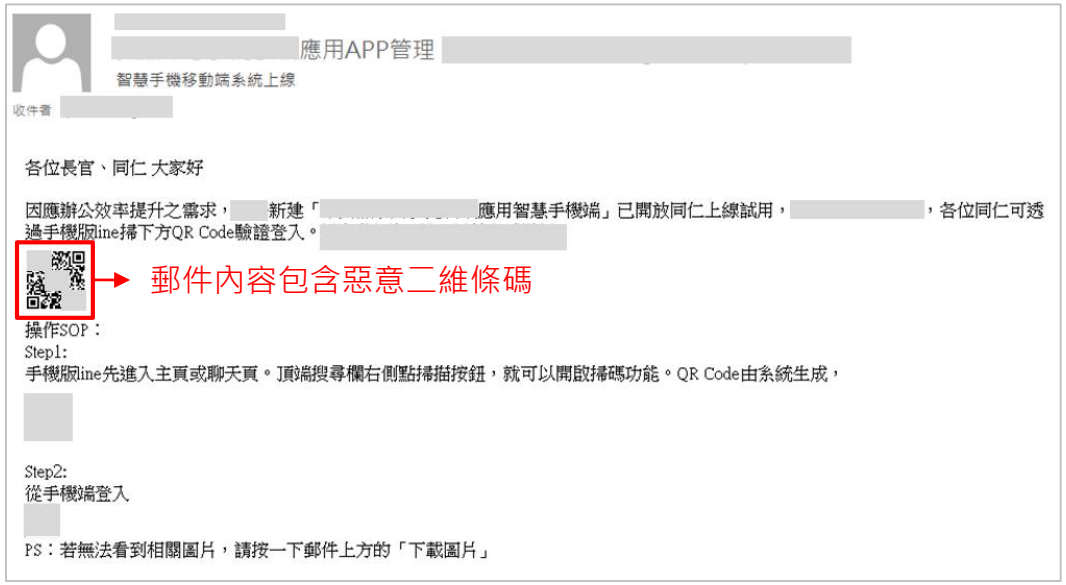
- 確認郵件附檔屬性或檔名後才點擊檔案，若檔名存在異常字元(如pdf.zip, pdf.exe, lnk)，請提高警覺

釣魚郵件社交工程攻擊案例

國家資通安全研究院
National Institute of Cyber Security

案情提要

- 駭客偽冒政府機關電子郵件，利用智慧手機系統上線等主旨，引誘收件者以行動裝置掃描惡意二維條碼(QR Code)
- 掃描後將連線至偽冒之登入頁面，要求收件人輸入帳號與通行碼
- 釣魚網頁無論輸入正確與否，皆跳轉至合法網站頁面，以降低收件人戒心



防護建議

- 加強宣導提升人員資安意識，勿掃描未知來源之二維條碼
- 多加注意透過二維條碼訪問之網站，可能包含利用漏洞或竊取資料之惡意程式碼

網路釣魚社交工程攻擊案例

案情提要

- 機關同仁瀏覽線上免費影音網站(楓X網)時，出現「我不是機器人」視窗，顯示「如果你不是機器人，請點擊下面按鈕」等資訊，點擊後即觸發惡意程式下載並執行

- 同仁執行程式後，即遭植入勒索軟體，導致個人電腦及NAS分享目錄檔案遭勒索軟體加密
- 機關立即將受害駭電腦中斷連線與封存，並將同業務組室斷網、關閉NAS分享目錄，並還原至前一天備份檔案

防護建議

- 加強宣導提升人員資安意識，勿隨意瀏覽與公務無關之網站
- 採「3-2-1原則」定期備份檔案，3份備份檔、2種不同備份方法及1份異地存放

網通設備產品漏洞攻擊(1/4)

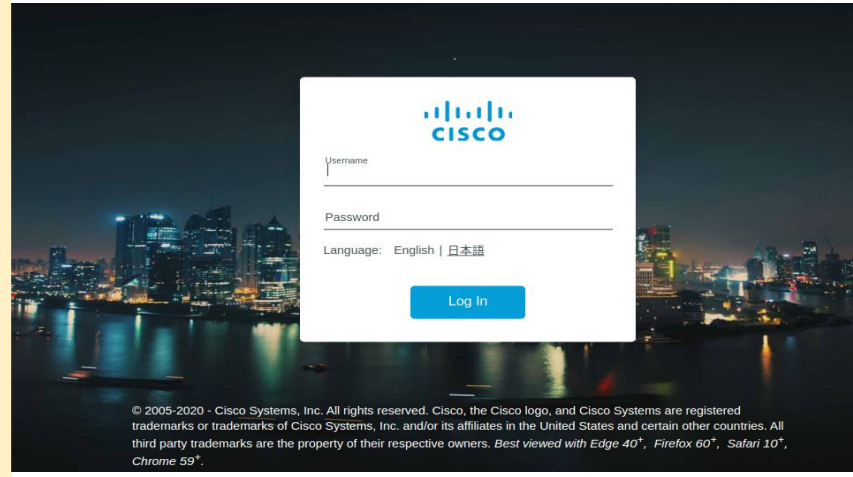
國家資通安全研究院
National Institute of Cyber Security

案情提要

- 資安院偵測發現多個公務機關Cisco設備存在嚴重漏洞(CVE-2023-20198)
- 透過原廠釋出之檢測方式，確認已遭駭客利用，共發佈9筆警訊
- 10/20發佈漏洞預警(NICS-ANA-2023-0000453)通知各機關應處

漏洞說明

- Cisco IOS XE之網頁介面允許遠端攻擊者在未經身分鑑別之情況下，新增高權限帳號，以此控制受影響之系統
- 若啟用網頁介面(Web UI)功能皆會受到影響，包含**交換器、無線網路控制器、無線基地台及路由器**等



網通設備產品漏洞攻擊(2/4)

國家資通安全研究院
National Institute of Cyber Security

防護建議

- 思科官方網站已針對部分型號設備公告修補程式，須儘速安裝
- 採用非網頁UI介面(關閉HTTP Server、HTTPS SERVER，或設定存取白名單)

官方檢測資訊

- Cisco官方與其所屬威脅情報組織Talos，釋出3種檢測方式

1

傳送一個特定HTTP POST至Cisco設備，若設備conf遭竄改，就會回傳16進位字串

```
D:\>curl -k -X POST "https://[redacted]/webui/logoutconfirm.html?logon_hash=1"
[redacted]45c815c4cc5f4

D:\>curl -k -X POST "https://[redacted]/webui/logoutconfi
/1010202301/
```

異常回傳畫面

網通設備產品漏洞攻擊(3/4)

2 由原檢測方式改進，於Http請求標頭新增授權驗證碼，以因應變種惡意程式規避原始檢測方式

```
❯ curl -k -H "Authorization: 0ff4fbf0ecffa77ce8d3852a29263e263838e
9bb" -X POST "http://2[redacted]54:80/webui/logoutconfirm.html?lo
gon_hash=1"

<!DOCTYPE html>
<html>
```

正常回傳畫面

```
❯ curl -k -H "Authorization: 0ff4fbf0ecffa77ce8d3852a29263e263838
e9bb" -X POST "http://2[redacted]9:80/webui/logoutconfirm.html?
logon_hash=1"

adcbf66a5aada0f8de
```

異常回傳畫面

資料來源：https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/

網通設備產品漏洞攻擊(4/4)

3 使用者存取設備網頁根路徑時，惡意程式會偽照並回應 404 Not Found 頁面，而正常未被植入程式設備會自動載入javascript程式跳轉至網頁登入路徑

```
❯ curl -k "http://2[redacted]1:80/%25"

<script>window.onload=function(){ url ='/webui';window.location.hr
ef=url;}</script>%
```

正常回傳畫面

```
❯ curl -k "http://[redacted]49:80/%25"

<html>
<head><title>404 Not Found</title></head>
<body>
<center><h1>404 Not Found</h1></center>
<hr><center>openresty</center>
</body>
</html>
```

異常回傳畫面

資料來源：https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/

網通設備儲存日誌空間不足

國家資通安全研究院
National Institute of Cyber Security

案情提要

- 資安院偵測發現多個公務機關設備對外下載木馬程式HiatusRAT，因設備紀錄保存不足或無紀錄功能導致難以進行根因調查
- 經機關調查後發現連線設備多為網通設備(路由器、防火牆)，受駭設備多久未進行韌體/軟體更新，舊版本存在漏洞遭利用

設備類型	廠牌數量	通報件數
路由器	1	3
防火牆	1	15
無線基地台	2	2
郵件伺服器	1	1

※112年統計資料

防護建議

- 定期檢視並更新設備系統/韌體版本
- 採購具有紀錄功能之設備
- 建立健全日誌保存機制，以利異常事件發生時之根因調查

產品漏洞攻擊導致帳密外洩(1/2)

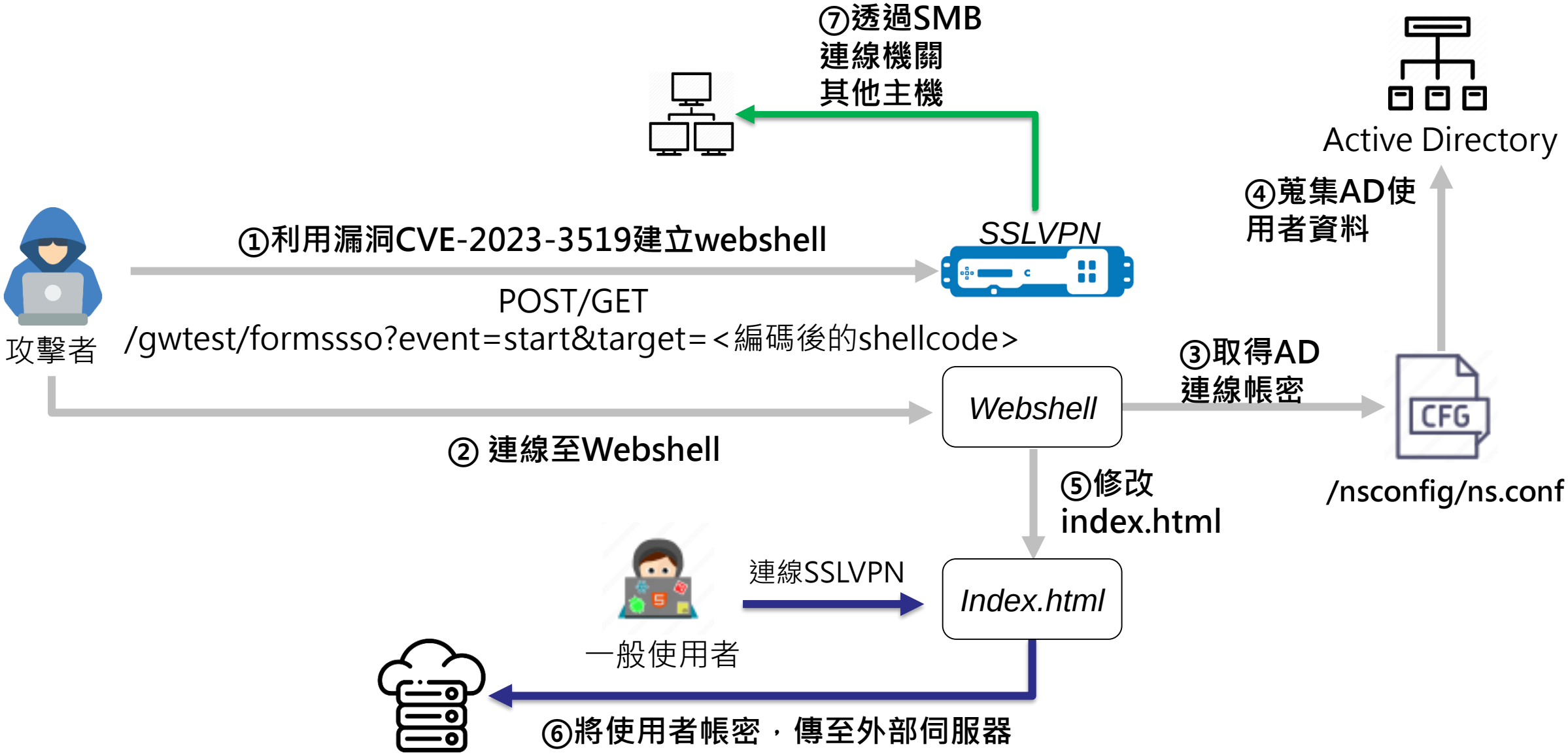
案情提要

- 機關防火牆發現大量異常連線，SSL VPN設備發送大量SMB封包
- 經查SSL VPN設備存在安全性漏洞(**CVE-2023-3519**)，攻擊者可利用漏洞上傳Webshell、探測腳本
- 在設備中取得可以連線到AD帳密檔，並透過ldapsearch查詢使用者訊息
- 竊取被駭期間連線SSLVPN使用者帳密

防護建議

- 及時更新或套用相關修補程式
- 及時更新特徵碼，透過防護設備阻擋攻擊
- 隔離外部設備網段，避免攻擊擴散

產品漏洞攻擊導致帳密外洩(2/2)

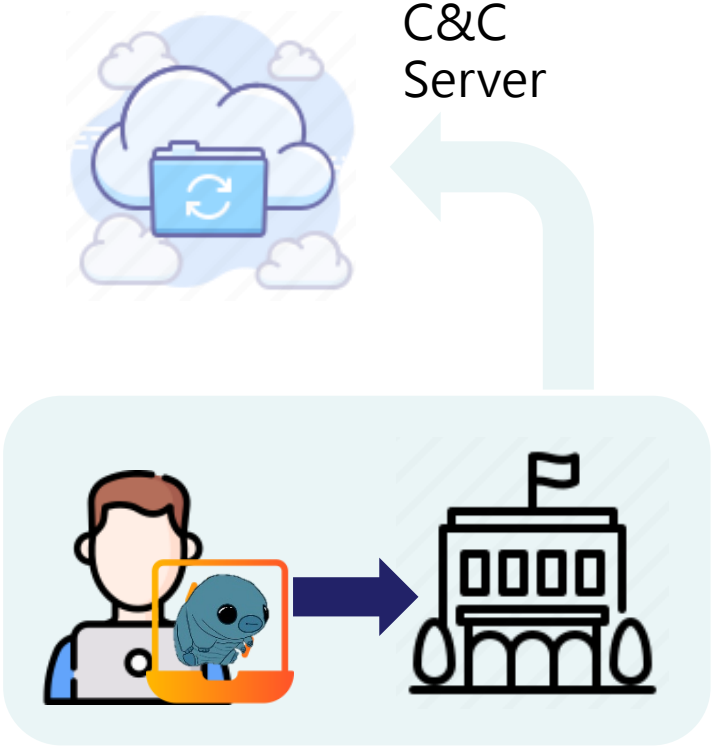


供應鏈廠商維護環境或管理疏失(1/3)

國家資通安全研究院
National Institute of Cyber Security

案情提要

- 廠商攜帶設備至機關進行維護作業，機關允許該設備連線至機房網路，待設備接上網路並操作一段時間後，資安院即發現**符合特定惡意程式行為之連線**
- 機關收到通知後，**即時將廠商設備斷網**，經查後未對機關設備造成進一步為害



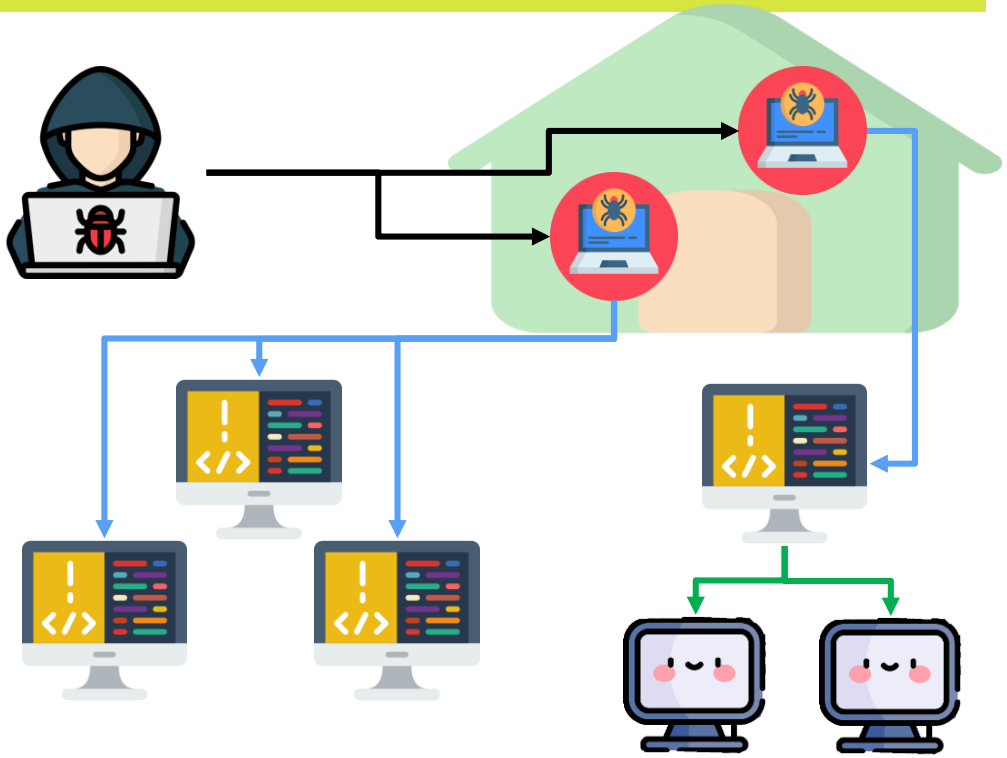
防護建議

- 廠商應恪守機關資通安全政策及委外廠商管理相關規範要求
- 攜帶之設備或工具應確保安全無虞，方可連線至機關內部網路

供應鏈廠商維護環境或管理疏失(2/3)

案情提要

- 機關發現多個外部觀測站設備，被維護廠商IP/帳號遠端桌面登入後執行勒索軟體，造成資料被加密無法存取使用
- 遭感染的觀測站又連結到其他觀測站，以致被加密範圍擴大



防護建議

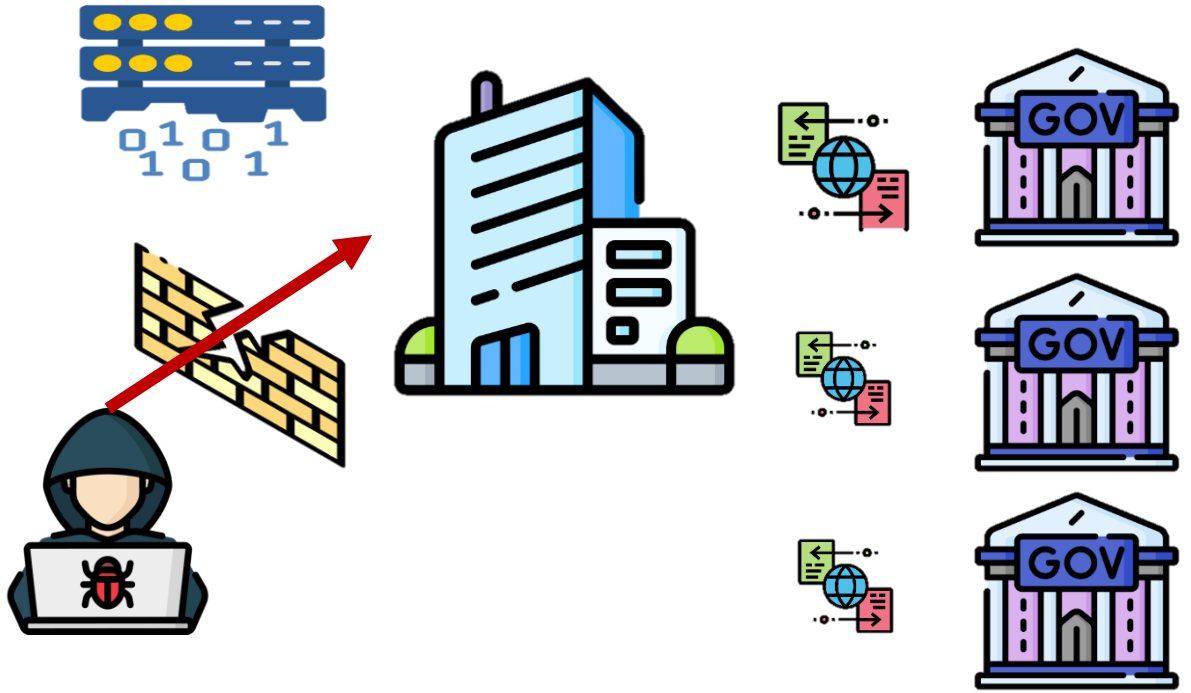
- 遠端維護作業應採「原則禁止、例外允許」方式進行，如開放遠端存取，應以短天期為限，並建立連線行為管理機制
- 維護廠商使用之密碼，亦應依照機關資通安全相關程序，定期變更

供應鏈廠商維護環境或管理疏失(3/3)

國家資通安全研究院
National Institute of Cyber Security

案情提要

- 機關因委請廠商執行系統開發作業，以致廠商持有機關相關業務資料
- 廠商端防護作業未落實，導致位於廠商端之機關資料外洩



防護建議

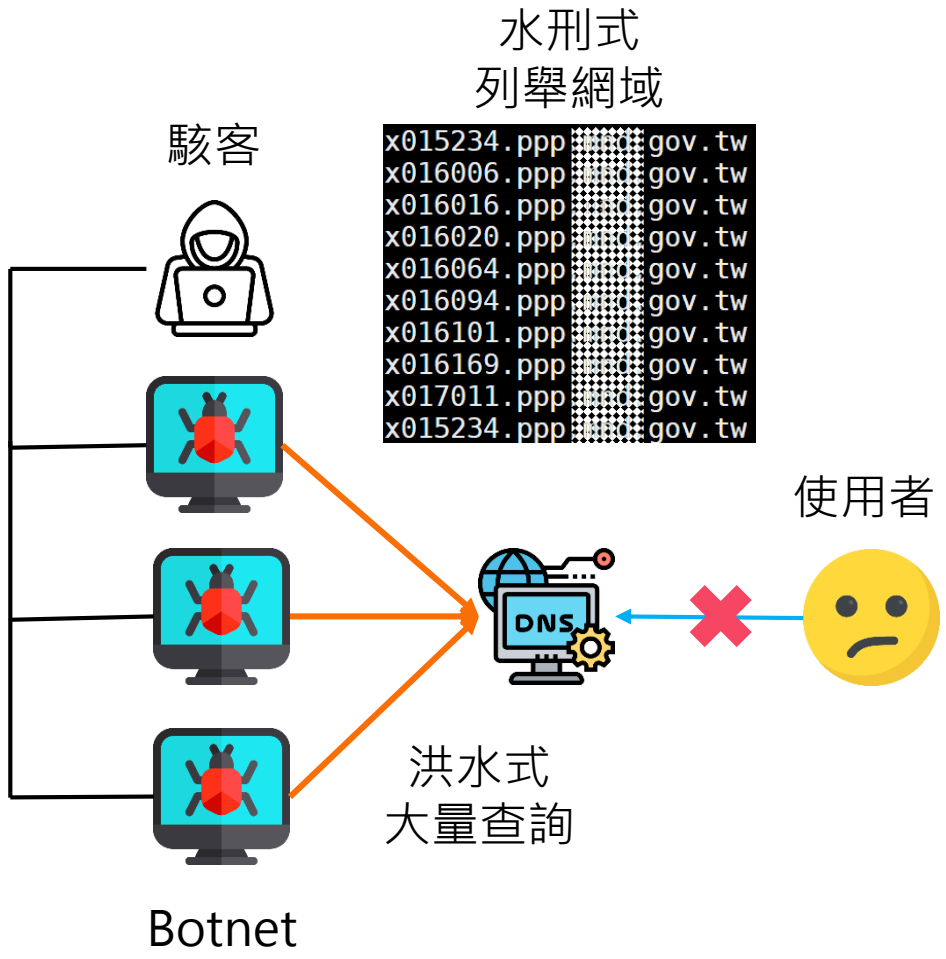
- 廠商如欲於其場域內建置測試環境，應依機關之資安責任等級，設置對應之防護、必要檢測及採白名單限制存取來源及帳號
- 所收集之資料使用完畢，應依機關程序要求，徹底刪除並留存刪除過程

政府機關DNS遭DDoS攻擊案例

國家資通安全研究院
National Institute of Cyber Security

案情提要

- 機關對外服務網站無法正常提供服務，經分析DNS遭受DDoS攻擊
- 遭受混合式DNS攻擊
  - 洪水攻擊(Flood Attack)
  - 水刑式攻擊(DNS Water-torture)
- 攻擊期間共查詢約1000萬(10,160,541)個網域名稱，14小時內共計查詢次數約1億5千400萬次



防護建議

- 採購流量清洗服務
- 限制查詢次數，並避免成為Open Resolver

政府機關資安防護強化重點

- 強化偵測防護以因應資安威脅
- 強化社交工程郵件防範
- 落實設備定期更新檢視暨執行
- 落實委外管理降低供應鏈風險

強化偵測防護以因應資安威脅(1/3)

A、B級公務機關須於112年8月23日前完成端點偵測及應變機制導入作業，納入資通安全威脅偵測管理機制監控範圍，並依主管機關指定方式提交偵測資料

端點偵測及應變機制	一、 初次受核定或等級變更後之二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。 二、 本辦法中華民國一百十年八月二十三日修正施行前已受核定者，應於修正施行後二年內，完成端點偵測及應變機制導入作業，並持續維運及依主管機關指定之方式提交偵測資料。

強化偵測防護以因應資安威脅(2/3)

- EDR偵測告警，經確認為資安事件時，由SOC依規定格式透過現有聯防監控資料回傳管道提交至主管機關
  - 回傳內容主要以惡意程式資訊為主，藉以強化事件關聯分析，掌握潛在攻擊來源

強化偵測防護以因應資安威脅(3/3)

- 落實端點偵測與應變機制導入，相關資訊可參考國家資通安全研究院官方網站「端點偵測及應變機制 (Endpoint Detection and Response，簡稱EDR) 」專區
  - 說明文件
  - 回傳格式範本
  - 相關測試或正式回傳方式

端點偵測及應變機制(EDR)

端點偵測及應變機制(Endpoint Detection and Response, 簡稱EDR)主要目的為偵測端點系統上異常活動，以期能及早發現駭客活動跡象，降低後續可能引發之資安風險。本專區提供EDR議題相關資源與常見問題，協助機關落實資通安全管理法應辦事項之法遵要求。
目前正與各SOC進行資料回傳的連通測試，所有A、B級機關須在112年8月23日前完成EDR導入，相關的時程規劃請參考端點偵測及應變機制資料回傳規劃說明文件。
有任何EDR議題相關問題，歡迎來信至 edwardchen@nics.nat.gov.tw 詢問！

備註：
持續接受EDR情資分析單之聯通測試，惟測試方式經調整後，欲測試廠商請將測試檔案寄至 edwardchen@nics.nat.gov.tw測試。
此外，目前已接受機關回傳EDR情資分析單，正式資料仍透過聯防監控的FTP進行資料傳送，勿將正式情資分析單透過MAIL寄送!

相關文件與表單 | FAQ

端點偵測及應變機制資料回傳規劃說明文件
端點偵測及應變機制資料回傳規劃說明_1120327.pdf
SHA256:E865E2D122CCA437EB497273F429EDD651AF68EF747529395A51C3196D21ED9B

情資分析單STIX文件範本
情資分析單_端點偵測及應變機制_1120104.rar
SHA256:1DCE08CB6D7538A751F94F9F7EDBE00D6785B9709A3D834A5CCC20834EEA4062

強化社交工程郵件防範

- 避免開啟非公務相關郵件，降低社交工程攻擊威脅
- 應建立電子郵件過濾機制，並加強郵件驗證機制與保留郵件日誌，以利溯源分析，例如密碼暴力破解登入或其他異常活動跡象
- 定期或不定期執行社交工程演練，辦理資安認知教育訓練，強化人員識別與判斷社交工程郵件之能力

確認信件來源

- 確認寄件者、寄件來源IP、附件檔案及信件內容(如網路連結)

設置垃圾郵件過濾設備

- 落實資通安全防護應辦事項，設置電子郵件過濾機制

保護資訊設備安全

- 定期進行系統安全性檢測，注意個別系統之安全修補與病毒碼更新

定期演練

- 藉由演練強化人員防護意識

落實設備定期更新檢視暨執行

國家資通安全研究院
National Institute of Cyber Security

強化資產盤點與漏洞修補

- 強化資產盤點與監控機制，即時掌握資通訊設備與相關資產資訊
- 隨時注意資通訊設備漏洞更新情況與相關公告，並儘速完成漏洞修補作業

強化存取控制管理

- 避免開放於公開網際網路，透過白名單限制存取來源
- 避免使用預設密碼/弱密碼，並定期變更密碼

確認日誌記錄功能

- 確認設備可使用之日誌記錄功能與保存項目
- 評估日誌可保存期限並落實儲存

落實委外管理降低供應鏈風險

- 委外辦理資通系統之建置、維運或資通服務，應要求廠商配合資通安全管理法及其子法之規定，符合委託機關所屬資通安全責任等級之要求，落實防護應辦事項，以因應資通安全威脅情勢變化

機關應辦理

- 選擇適任之受委託廠商/人員
- 制定與落實委外系統或服務之管理措施
- 監督委外系統或服務之資安維護情形

委外廠商/人員 應配合

- 系統防護需求分級原則
- 資通系統防護基準
  - 系統發展生命週期(SSDLC)
  - 帳號管理 / 最小權限
  - 漏洞修復 / 系統監控
  - 事件紀錄 / 日誌儲存容量

強化通報資料完整性與正確性

通報單常見錯誤填報情形

國家資通安全研究院
National Institute of Cyber Security

- 通報流程概分為通報、應變處置及結報，常見錯誤填報情形
  - 將事件原因視為事件類型，或將受駭情形視為事件原因
  - 未做事件調查，將推測結果視為事件原因

通報 → **應變處置** → **結報**

通報階段

基本資料	機關名稱、通報人、是否代通報
發生過程	**事件分類與異常狀況**、事件說明
事件等級	機密性、完整性、可用性
外部支援	是否支援、期望支援項目

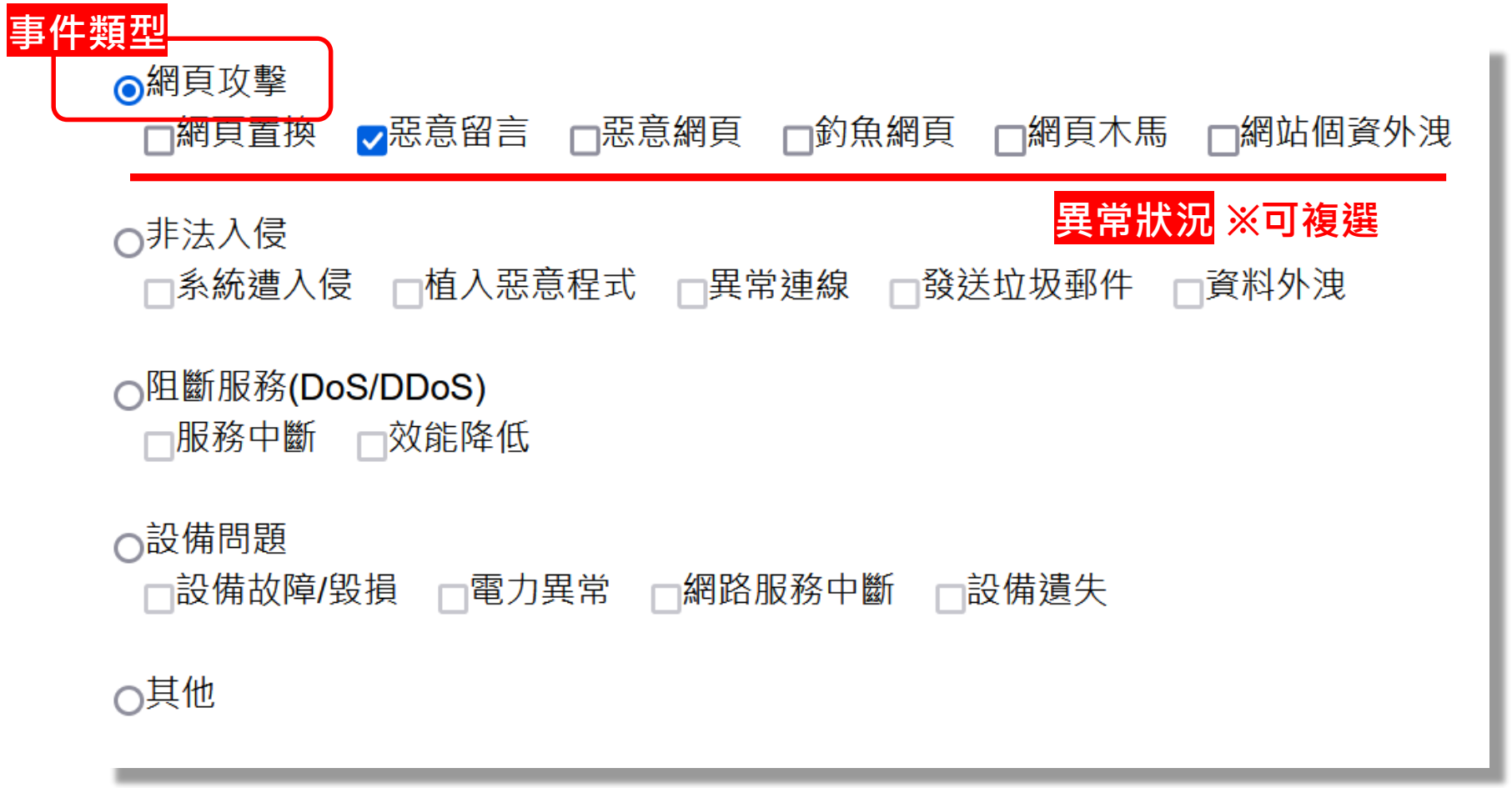
結報階段

事件調查	設備數量、IP、作業系統等
事件發生原因	作業系統漏洞、弱密碼等
補強措施	系統更新、教育訓練等

通報網站事件類型與異常狀況(1/3)

國家資通安全研究院
National Institute of Cyber Security

- 為利非資安專業人員勾選事件類型，臚列事件觀察到「異常狀況」，做為事件類型判別方法



通報網站事件類型與異常狀況(2/3)

網頁攻擊	網頁置換	內容遭非法篡改
	惡意留言	網頁留言版遭張貼情色資訊、煽動或教唆他人犯罪之留言
	惡意網頁	網頁遭非法植入可執行程式碼，導致瀏覽者遭入侵
	釣魚網頁	系統遭放置可控制網站之網頁型木馬程式
	網頁木馬	網頁含有竊取他人資訊之偽冒頁面
	網站個資外洩	網站不當公開個人敏感性資料

非法入侵	系統遭入侵	發現系統遭入侵(如：異常設定)
	遭植入惡意程式	主機發現惡意程式(如：後門程式、木馬程式、蠕蟲、病毒等)
	異常連線	內部主機對外不正常連線
	發送垃圾郵件	郵件伺服器對外發送垃圾郵件
	資料外洩	業務資料遭打包

通報網站事件類型與異常狀況(3/3)

阻斷服務	服務中斷	系統遭阻斷服務攻擊，資源耗盡導致系統服務中斷
	效能降低	系統遭阻斷服務攻擊，導致系統效能降低，超過機關可容忍範圍

設備問題	設備毀損	資訊設備因老舊或其他不可抗力因素損毀，導致系統/服務中斷
	電力異常	因不正常供電，導致系統/服務運作停頓
	網路服務中斷	網路服務非預期中斷，導業機關系統/服務無法正常運作
	設備遺失	資訊設備因外部因素遺失

其他	非上述事件類型資安事件

常見錯誤填報情形-將事件原因視為事件類型

國家資通安全研究院
National Institute of Cyber Security

Q. 停電影響服務運作

台電無預警停電，導致機關資訊設備無法正常運作，影響機關日常業務運行

台電無預警斷電**並非自身設備故障**導致事件發生，事件類型選填「設備問題」是否妥適？

A：

- 設備因電力問題無法正常使用為當下設備異常狀況
- 台電無預警停電，為電力異常根因
- 事件類型應勾選「設備問題」(電力異常)

- 部分機關考量非自身設備故障/毀損，故通報其他事件類型
- 惟事件類型係以機關設備異常狀態進行識別

常見錯誤填報情形-將受駭情形視為事件原因(1/2)

國家資通安全研究院
National Institute of Cyber Security

Q. 資訊設備異常連線

機關接獲資安院警訊通知，資訊設備異常連線挖礦主機

經防毒軟體掃描，**發現電腦中毒**，判斷事件原因為電腦中毒

A：

- 資訊設備經防毒軟體掃描發現挖礦程式，為該事件觀察到異常狀況
- 因進一步釐清挖礦程式植入原因，例如安裝之錄影程式含挖礦軟體
- 事件原因應勾選「社交工程」

- 電腦中毒、當機或異常連線皆係資訊設備異常時可觀察到現象，應進一步釐清造成異常之原因
- 事件類型可參照警訊通知內容勾選

事件類型

☑非法入侵
☐系統遭入侵 ☑植入惡意程式 ☑異常連線 ☐發送垃圾郵件 ☐資料外洩

行政院國家資通安全會報技術服務中心

入侵事件警訊

發布編號	NCCST-INT[redacted]	發布時間	[redacted]
事件類型	可疑連線	發現時間	[redacted]
事件主旨	[redacted]年事務局內部設備有異常連線挖礦主機之行為		
事件描述	技服中心近期發現 貴單位設備[redacted])曾連線至挖礦主機(172.65.200.133,199.247.27.41)並存在報到行為特徵。		
手法研判	無		
	1.盤點與檢視相關設備系統，判定是否遭入侵並植入惡意程式，導致可疑連線行為。		

常見錯誤填報情形-將受駭情形視為事件原因(2/2)

國家資通安全研究院
National Institute of Cyber Security

Q. 資訊設備遭異常登入

機關接獲SOC廠商通知，資訊設備遭異常登入

經查發現外部IP成功利用委外廠商VPN帳號，登入跳板機後，再登入機關其他應用系統，判斷事件原因為**廠商VPN帳號密碼遭盜用**

A：

- 帳號密碼遭盜用為該事件觀察到異常狀況
- 應進一步釐清帳號密碼外洩管道，例如委外廠商資訊設備遭入侵植入鍵盤側錄器
- 事件原因應勾選「廠商維護環境或管理疏失」

事件類型

- ☑非法入侵
- ☑系統遭入侵 ☐植入惡意程式 ☑異常連線 ☐發送垃圾郵件 ☐資料外洩

Q. 電子郵件帳號密碼洩漏

機關接獲資安院警訊通知，機關電子郵件帳號密碼洩漏，對外寄發主旨含帳密資訊郵件

- 經查事發9週內登入紀錄，未發現有該帳號登入情形
- 經測試確認，未登入狀況下，可透過SMTP利用該帳號寄送郵件
- 事件原因填寫**偽冒寄件者發信**

A：

- 偽冒寄件者發信為該事件觀察到異常狀況
- 應進一步釐清帳號密碼外洩管道
- 若查無外洩管道，事件原因應勾選「無法確認事件原因」

常見錯誤填報情形-未做事件調查，將推測結果視為事件原因

- 通報單資料應符合實際狀況
  - 若未盡調查事宜，事件原因應填寫「無法確認事件原因」(受限於資安人力/預算無法調查、逕行重建無法調查)
  - 進行根因調查，並提出紀錄分析情形

Q. 資訊設備異常連線

機關接獲資安院警訊通知，資訊設備異常連線挖礦主機

廠商僅說明事發原因為弱密碼，未提供更多資訊，並說明設備開放遠端連線，表示帳號密碼為預設值，故推測事件原因為弱密碼

A：
- 廠商未能說明調查情形，例如日誌紀錄分析、異常登入情形，未有足夠資訊推判事件發生原因
- 事件原因應勾選「無法確認事件原因」(受限於資安人力/預算無法調查、逕行重建無法調查)

Q. 資訊設備異常連線

機關接獲資安院警訊，通知機關「資訊設備產生符合HiatusRAT網通設備惡意程式行為之連線」

連線設備為防火牆(QNO SVM8641)，**並將設備重置、韌體更新至最新，後續即未再觸發異常連線**

機關表示**廠商查看過後表示「推測」應是舊版本有漏洞被利用所致**

A：
- 本案未具體跡證顯示透過韌體漏洞進行入侵
- 事件原因應勾選「無法確認事件原因」(事件調查後仍無法確認原因)為佳

其他填報案例(1/2)

- 事件觀察到「異常狀況」若涉及多個事件類別，機關可自行認定事件類型

機關自行發現網站伺服器遭植入**網頁木馬**與**其他惡意程式**，
並發現資訊設備**異常連線**中繼站

檢視
系統

檢視
網站

建議之事件類型

非法入侵

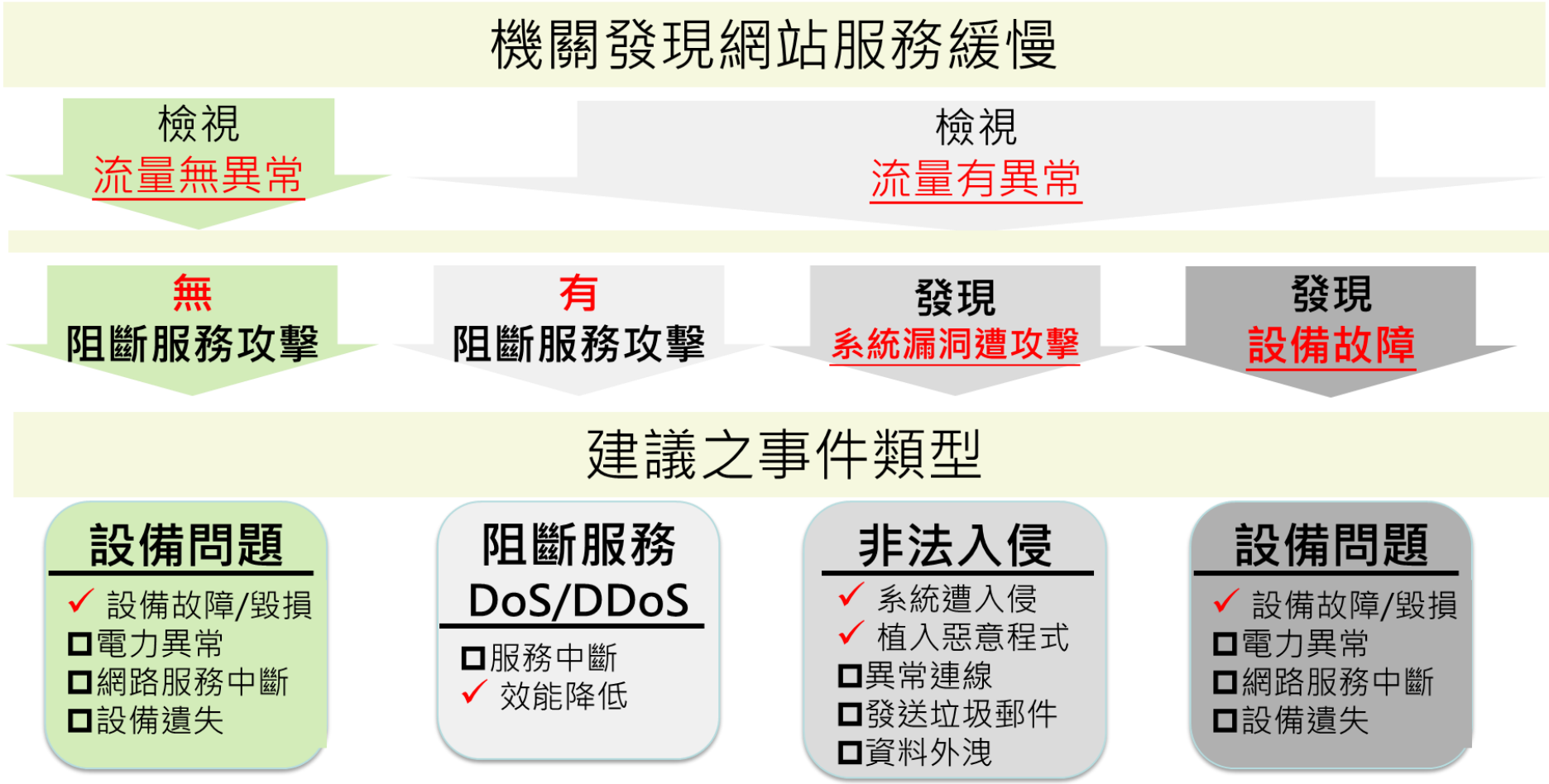
✓ 系統遭入侵　✓ 異常連線　☐資料外洩
✓ 植入惡意程式　☐發送垃圾郵件

網頁攻擊

☐網頁置換　☐惡意網頁　✓ 網頁木馬
☐惡意留言　☐釣魚網頁　☐網站個資外洩

其他填報案例(2/2)

- 系統異常或服務緩慢，通報當下尚無法判斷係否遭阻斷服務攻擊，建議勾選設備問題，待釐清後可再行調整事件類型



結論與建議(1/2)

- 社交工程攻擊仍為常見攻擊手法，機關應持續加強內部宣導，提升人員資安意識
  - 注意郵件來源正確性，慎防異常附件與連結
  - 注意個別系統之安全修補(含應用程式)與病毒碼更新

- 機關應落實資訊作業委外安全管理，敦促委外廠商遵守資安規範
  - 配合辦理系統防護需求分級原則與資通系統防護基準
  - 避免未經管制設備於機關環境中使用
  - 遠端維護作業應採「原則禁止、例外允許」方式進行
  - 如須開放遠端存取，應以短天期為限，並應建立連線行為管理機制

結論與建議(2/2)

- 關注資通訊設備漏洞情資，提升弱點防護能力，落實資安監控
  - 應隨時關注資通訊設備之情資(漏洞資訊、零日攻擊)，適時更新韌體版本或採行必要之防護設定
  - 導入端點偵測及應變機制，強化資安監控與防護，落實資安防禦縱深
  - 落實日誌保存作業，以利資安事件之鑑識分析

國家資通安全研究院
National Institute of Cyber Security

報告完畢
敬請指教

參考資料(1/2)

[1] ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[2] CVE-2023-20198 – Cisco IOS-XE ZeroDay, https://censys.com/cve-2023-20198-cisco-ios-xe-zeroday

[3] Gafgyt malware exploits five-years-old flaw in EoL Zyxel router, https://www.bleepingcomputer.com/news/security/gafgyt-malware-exploits-five-years-old-flaw-in-eol-zyxel-router

[4] Gartner Identifies Top Security and Risk Management Trends for 2022, https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

[5] 9th Annual State of the Software Supply Chain, https://www.sonatype.com/state-of-the-software-supply-chain/open-source-supply-and-demand

[6] New Veeam Research Finds 93% of Cyber Attacks Target Backup Storage to Force Ransom Payment, https://www.veeam.com/news/new-veeam-research-finds-93-percent-of-cyber-attacks-target-backup-storage-to-force-ransom-payment.html

參考資料(2/2)

[7] 勒索軟體Knight隱身於偽造的Tripadvisor投訴釣魚信件, https://www.ithome.com.tw/news/158281

[8] 2023 Global Report Ransomware Trends, https://www.veeam.com/ransomware-trends-report-2023

[8] https://www.cisa.gov/stopransomware/general-information#:~:text=Fend%20Off%20Phishing%20%3A%20Learn%20how,to%20better%20recognize%20phishing%20emails

[9] Introducing Cloudflare ‘s 2023 phishing threats report, https://blog.cloudflare.com/2023-phishing-report/

[10] The Tipping Point: Exploring the Surge in IoT Cyberattacks Globally, https://blog.checkpoint.com/security/the-tipping-point-exploring-the-surge-in-iot-cyberattacks-plaguing-the-education-sector

[11] The State of Ransomware 2023, https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf

[12] 會自我加密的新型勒索軟體 Cactus，讓防毒軟體及網路監控工具偵測不到，https://technews.tw/2023/05/12/new-cactus-ransomware-encrypts-itself-to-evade-antivirus/