區網網管會議

臺灣大學計資中心
李美雯
mli@ntu.edu.tw
3366-5010

大 綱

- 資安案例分享
  - ohSoft 軟體挖礦事件
  - CLDAP 反射式放大攻擊
  - 加密貨幣挖礦
  - 病毒式釣魚信件案例
  - 勒索恐嚇郵件攻擊
- 資通安全管理法

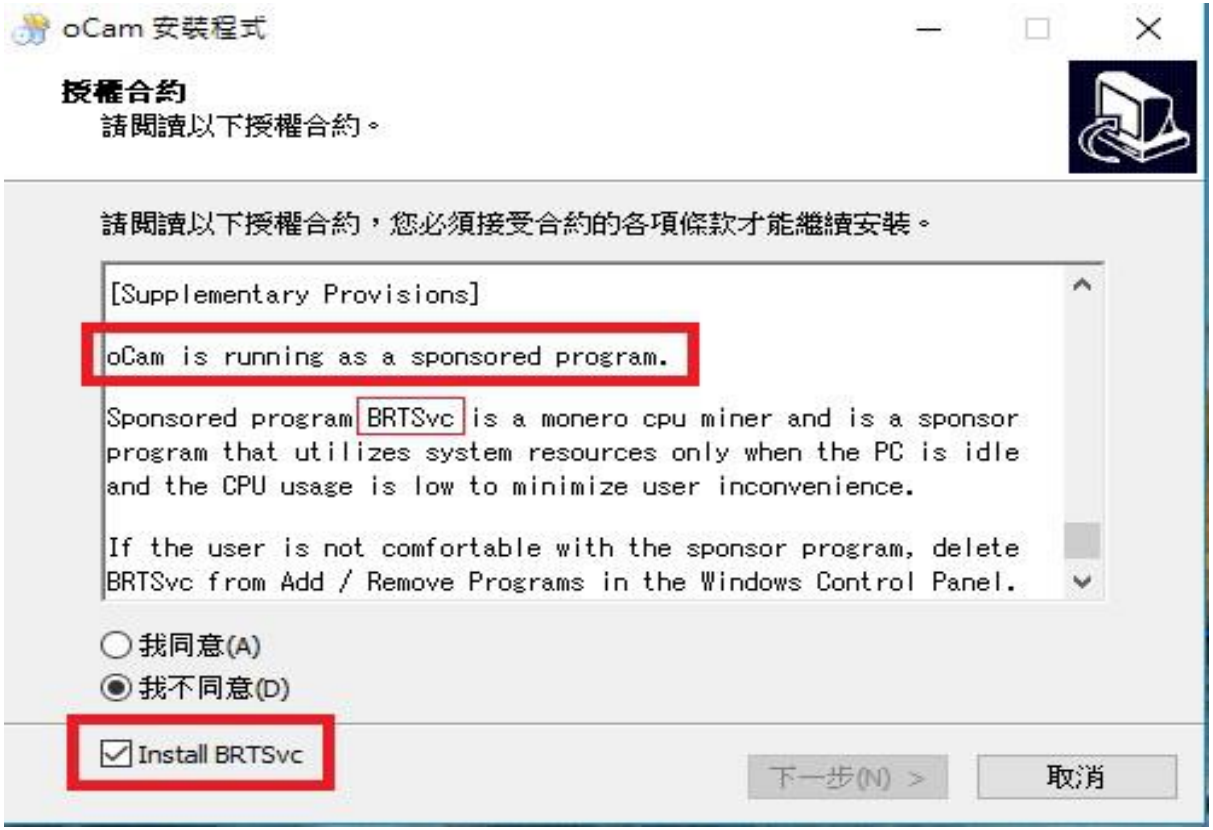
大 綱

- 資安案例分享
  - ohSoft 軟體挖礦事件
  - CLDAP 反射式放大攻擊
  - 加密貨幣挖礦
  - 病毒式釣魚信件案例
  - 勒索恐嚇郵件攻擊
- 資通安全管理法

ohSoft 軟體挖礦事件

- 臺大老師反應免費螢幕錄製軟體oCam夾帶挖礦程式 BRTSvc.exe，進而發現ohsoft旗下所有軟體(oCam、VirtualDVD、Secret Folder等)皆有此情況。

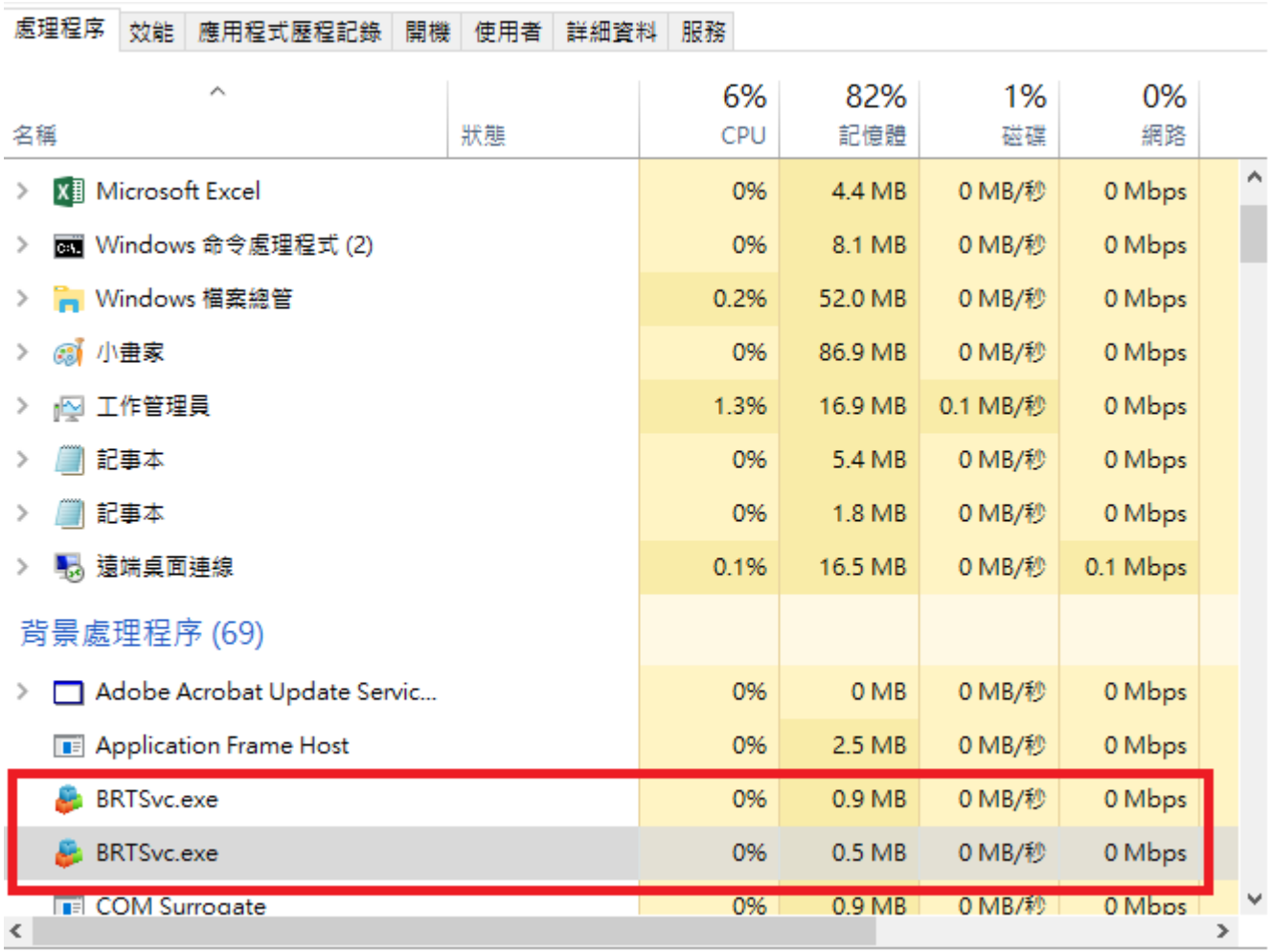
- 如下圖所示，oCam 安裝主程式的合約中，使用者除同意成為挖礦程式的贊助者，並且預設同意安裝挖礦程式BRTSvc.exe 。



出處:北區ASOC整理

ohSoft 軟體挖礦事件

挖礦程式BRTSvc.exe本身不會長時間佔用主機之網路或CUP



出處:北區ASOC整理

ohSoft 軟體挖礦事件

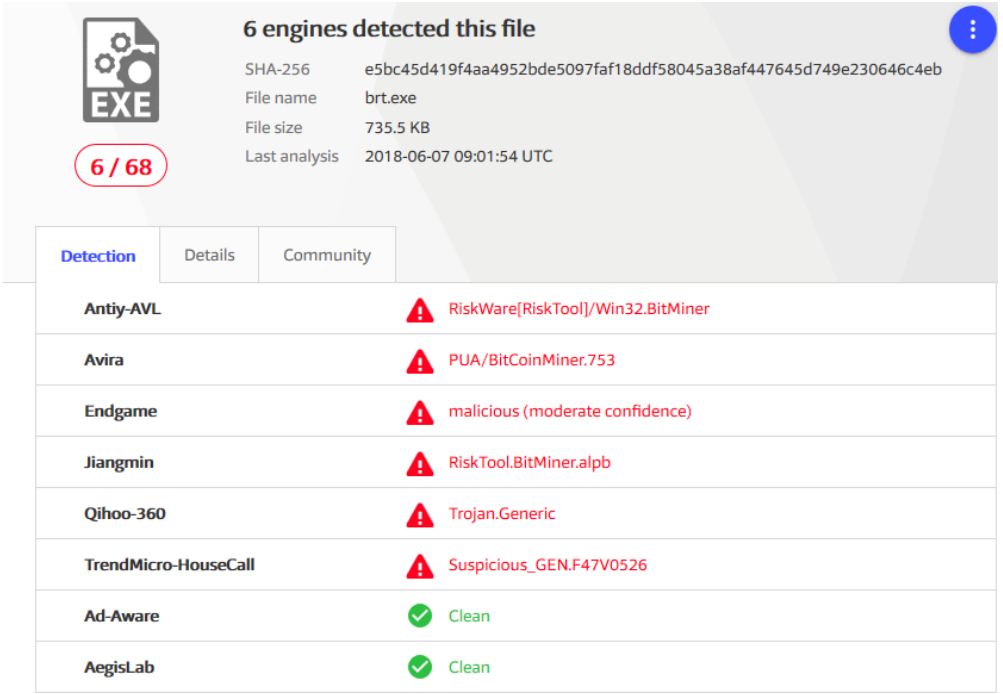
- 挖礦程式BRTSvc不會隨者主程式移除而移除，可利用新增/移除程式移除。
- 移除時建議打開工作管理員關閉相關程式，或是檢查是否被防毒軟體隔離，導致無法移除。

出處:北區ASOC整理

ohSoft 軟體挖礦事件

- **分析與建議**

針對此次oCam之挖礦程式，除使用者自行移除外，也可以用下列可偵測到之防毒進行掃毒



出處:北區ASOC整理

CLDAP 反射式放大攻擊

389 port (CLDAP、LDAP)

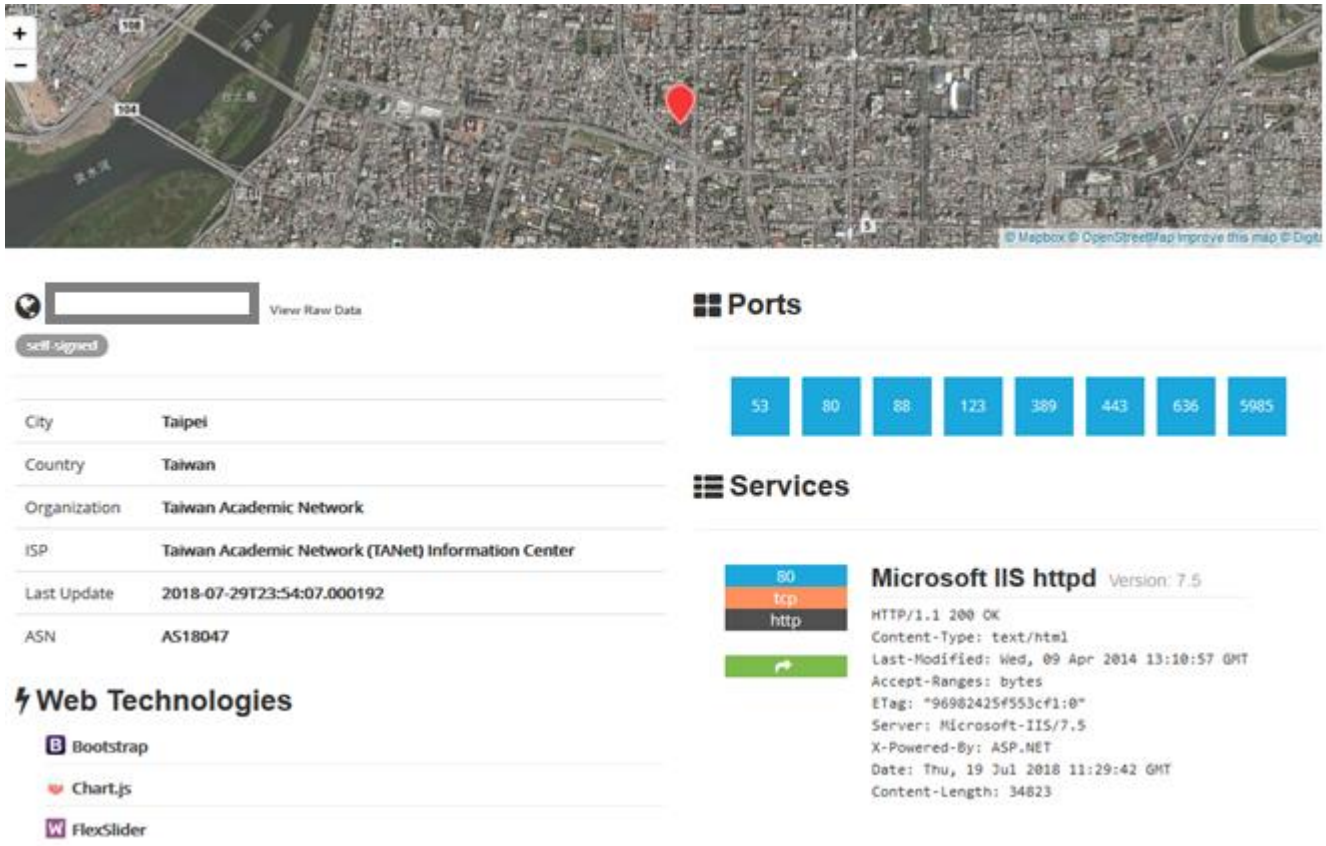
- LDAP (Lightweight Directory Access Protocol) 為AD上利用 TCP 389 PORT進行傳輸的協定。
- CLDAP (Connection-less Lightweight Directory Access Protocol)為AD上利用 UDP 389 PORT 進行傳輸的協定。
- Windows AD 的rootDSE，預設情況下是不需要權限，即可存取的。
- CLDAP反射式放大攻擊，最大放大倍率，可以高達50倍。

出處:北區ASOC整理

CLDAP 反射式放大攻擊

實測遭利用予攻擊之學校IP，進行rootDSE查詢。

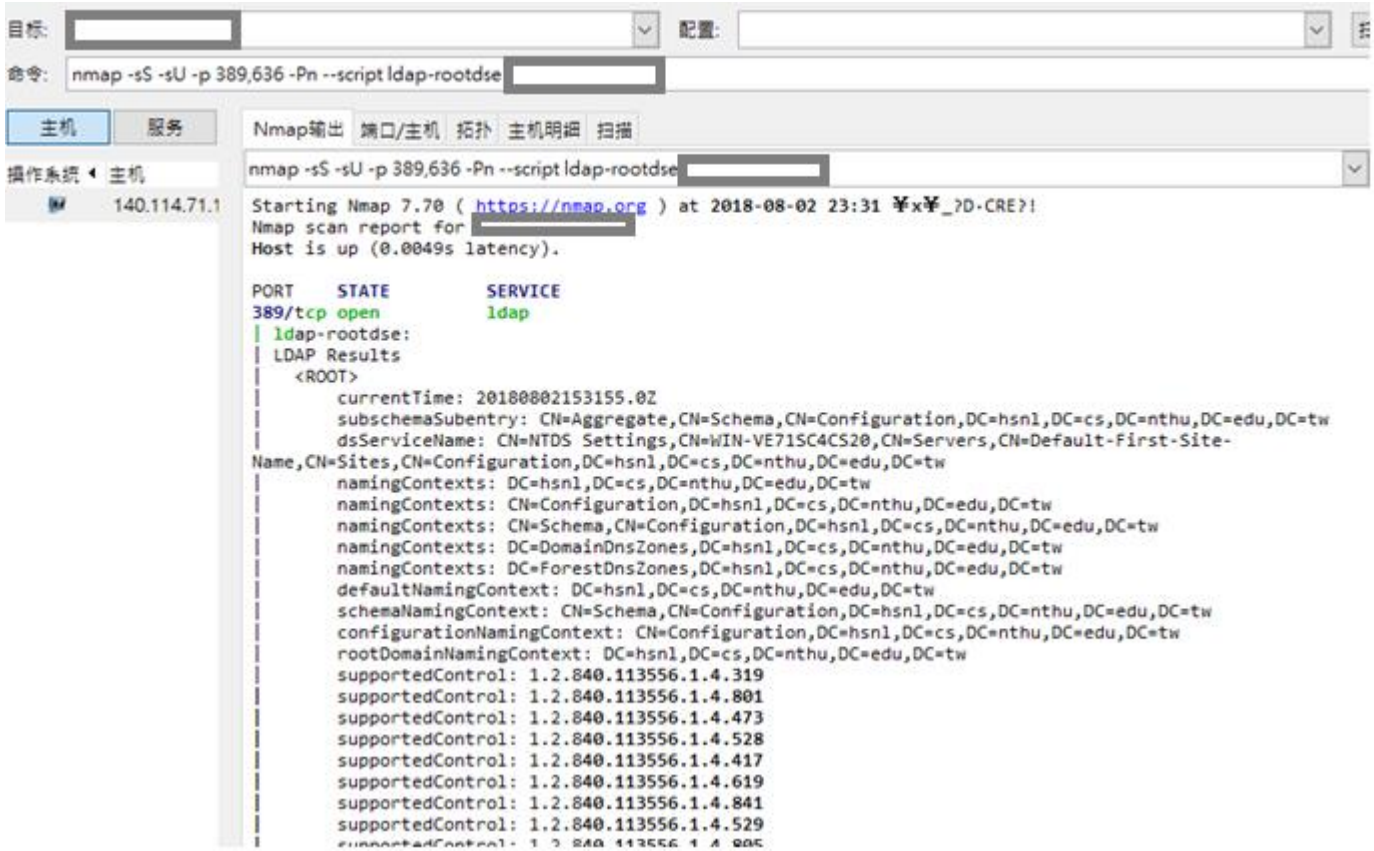
使用shodan進行搜索，確實能公開查詢到。



出處:北區ASOC整理

CLDAP 反射式放大攻擊

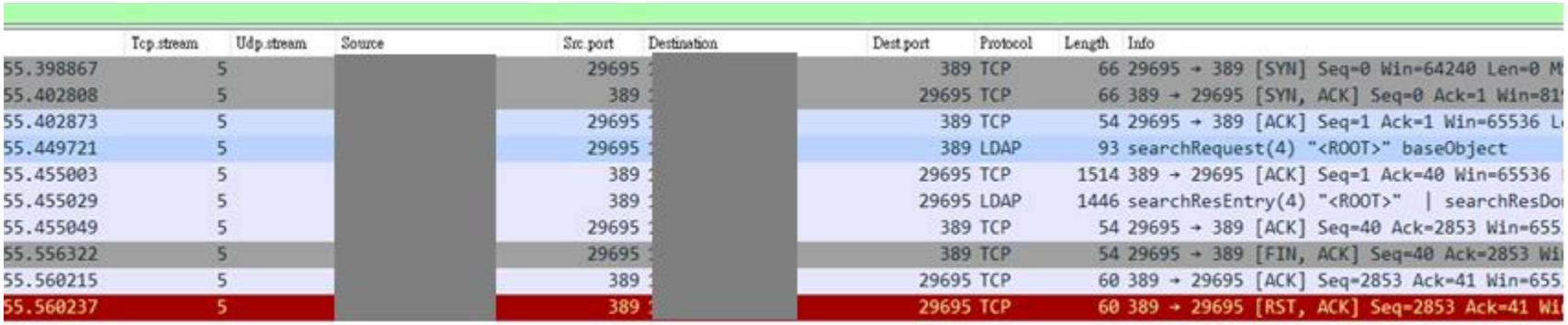
使用nmap進行掃描，也確實有資料回應



出處:北區ASOC整理

CLDAP 反射式放大攻擊

從封包的角度觀察，不到100 bytes的封包，可以造成近5000 bytes的回應封包，放大率至少有50倍以上。



	Tcp.stream	Udp.stream	Source	Src.port	Destination	Dest.port	Protocol	Length	Info
55.398867	5			29695		389	TCP	66	29695 → 389 [SYN] Seq=0 Win=64240 Len=0 M
55.402808	5			389		29695	TCP	66	389 → 29695 [SYN, ACK] Seq=0 Ack=1 Win=81
55.402873	5			29695		389	TCP	54	29695 → 389 [ACK] Seq=1 Ack=1 Win=65536 L
55.449721	5			29695		389	LDAP	93	searchRequest(4) "<ROOT>" baseObject
55.455003	5			389		29695	TCP	1514	389 → 29695 [ACK] Seq=1 Ack=40 Win=65536
55.455029	5			389		29695	LDAP	1446	searchResEntry(4) "<ROOT>" | searchResDo
55.455049	5			29695		389	TCP	54	29695 → 389 [ACK] Seq=40 Ack=2853 Win=655
55.556322	5			29695		389	TCP	54	29695 → 389 [FIN, ACK] Seq=40 Ack=2853 Wi
55.560215	5			389		29695	TCP	60	389 → 29695 [ACK] Seq=2853 Ack=41 Win=655
55.560237	5			389		29695	TCP	60	389 → 29695 [RST, ACK] Seq=2853 Ack=41 Wi

Udp.stream	Source	Src.port	Destination	Dest.port	Protocol	Length	Info
596	180.166.67.136	389		3779	CLDAP	1088	searchResEntry(1) "<ROOT>" searchResDone(1) success [37 res
	180.168.169.118				IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=34f3) [Reass
	180.166.128.18				IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=41f4) [Reass
611	180.168.169.118	389		3779	CLDAP	1452	searchResEntry(1) "<ROOT>" searchResDone(1) success [37 res
	180.166.47.250				IPv4	882	Fragmented IP protocol (proto=UDP 17, off=1480, ID=28f9) [Re
1281	180.166.47.250	389		3779	CLDAP	1514	searchResEntry(1) "<ROOT>" searchResDone(1) success [36
	180.169.127.29				IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=6be7) [Re
	180.168.119.52				IPv4	1450	Fragmented IP protocol (proto=UDP 17, off=1480, ID=7476) [Re
	192.192.135.200				IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=0b9e) [Re
992	192.192.135.200	389		61202	CLDAP	1181	searchResEntry(1) "<ROOT>" searchResDone(1) success [37

出處:北區ASOC整理

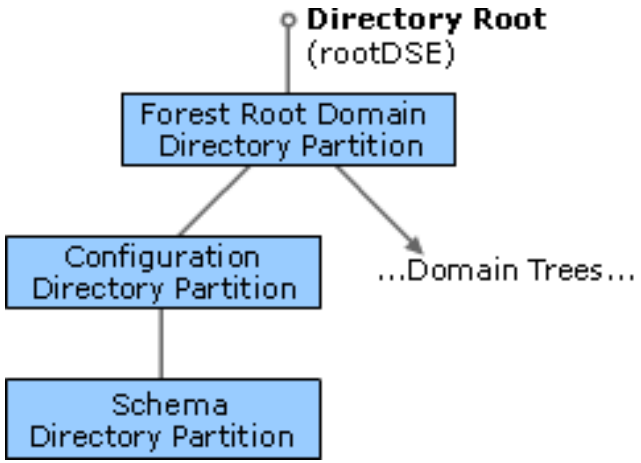
CLDAP 反射式放大攻擊

預防

- 使用者可架設防火牆進行ACL的控管
- 於設定檔中關閉**Anonymous Access**
- AD 應盡量避免暴露於Internet

CLDAP 反射式放大攻擊

補充：**rootDSE**



1. rootDSE 為AD的根目錄。
2. 供使用者查找路徑、其他相關設定。
3. 因AD在連線傳輸時，皆為TCP傳輸，占用不少connection數以及CPU效能，為了減輕AD負擔，允許使用者利用UDP (CLDAP) 查找AD根目錄。
4. AD本身設計，即僅提供於信任的環境中，供使用者做查詢。因此將AD暴露於網路上，又不做任何限制，會遭致資料外洩，及遭DDOS攻擊利用之風險。

參考來源：

1. https://technet.microsoft.com/zh-tw/library/ff700174.aspx
2. https://kb.iweb.com/hc/en-us/articles/115001073692-Guide-to-Microsoft-Active-Directory-rootDSE-C-LDAP-security-issues

釣魚信件案例

釣魚信件以「回覆(Reply)」型態發動攻擊，分析說明如下:

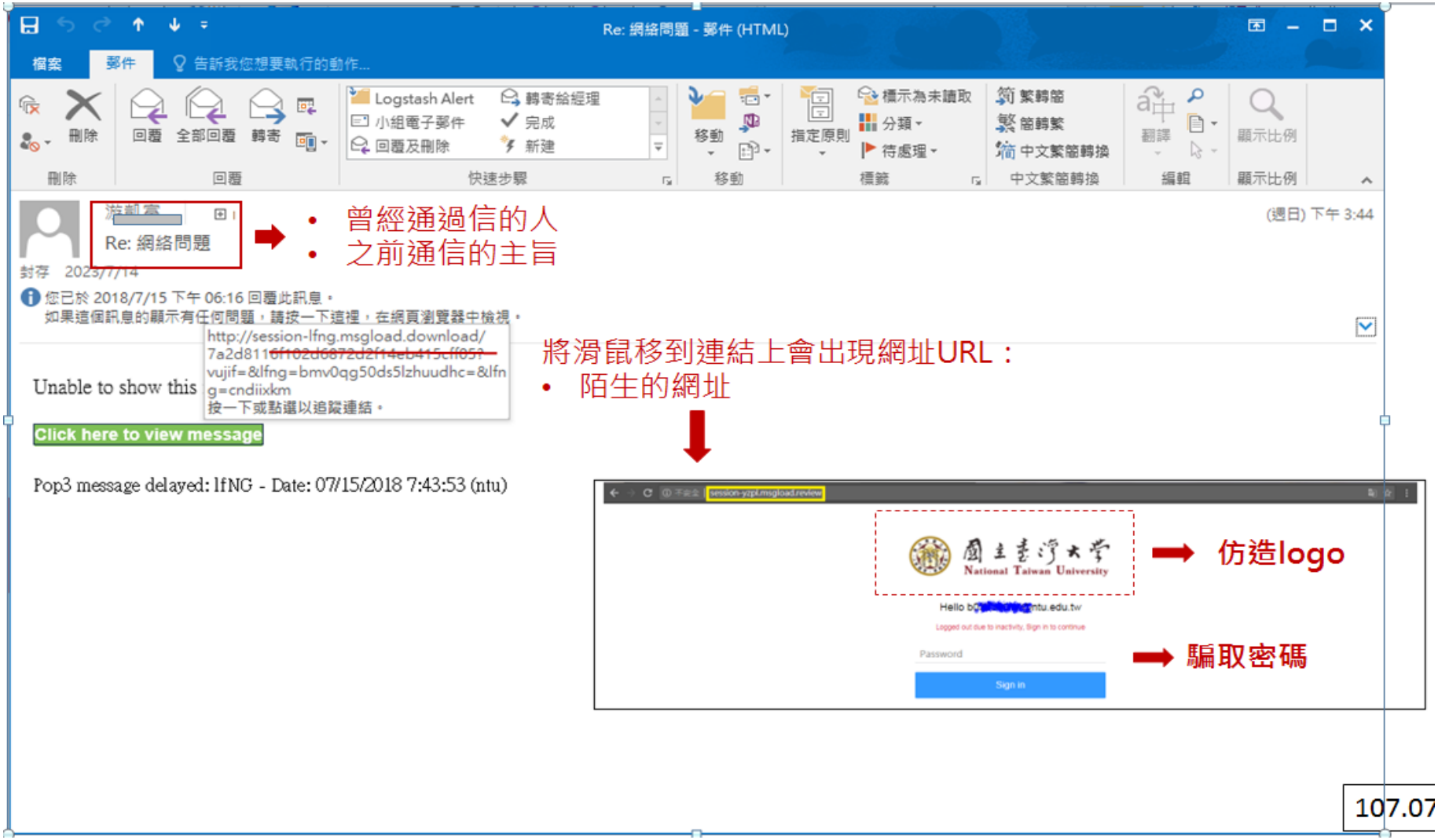
- 寄件者為曾經通過信的人
- 郵件主旨為之前通信的主旨

開啟信件時出現錯誤訊息「Unable to show this message」，誘使收件者點擊信件中的訊息按鈕「Click here to view message」(如圖一所示)。接著轉導至仿造的學校郵件網頁(如圖二所示)，讓不知情的收件者輸入自己的帳號及密碼，導致郵件帳密被盜取，形同中毒接續下一波的釣魚信攻擊。

釣魚信件內容

出處:北區ASOC整理

釣魚信件案例



釣魚信件深入分析

出處:北區ASOC整理

釣魚信件案例

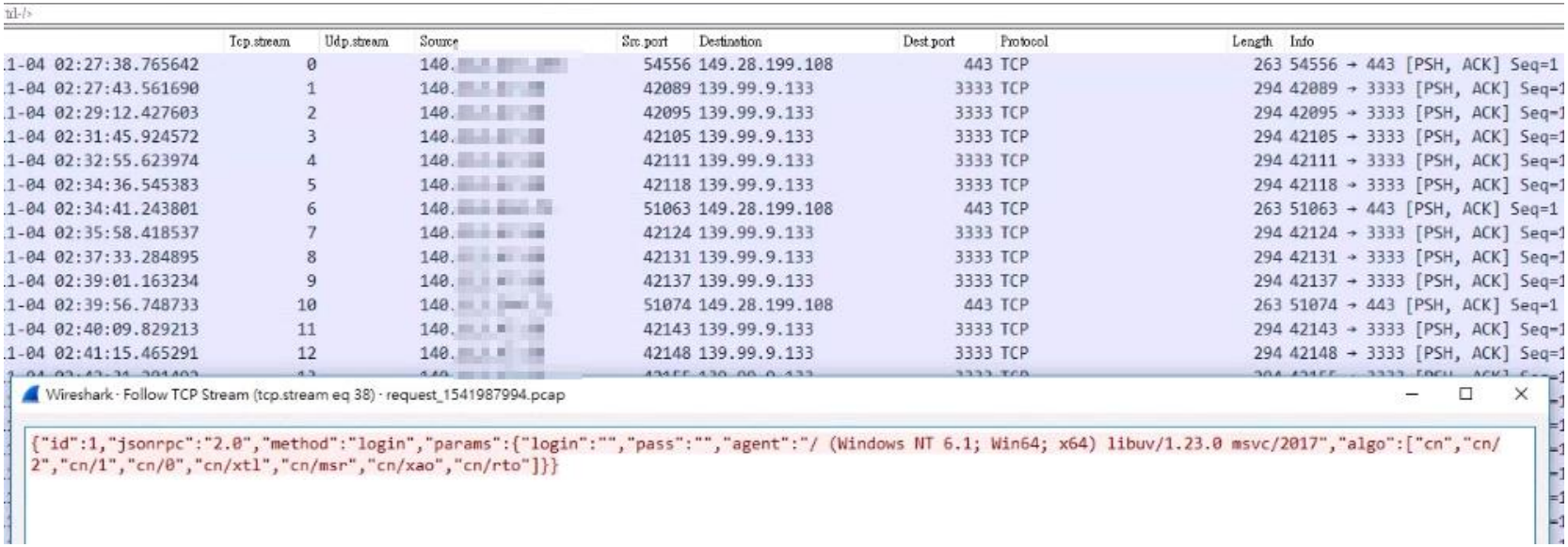
收到釣魚信件的建議措施:

- **勿理會該信件**，通知學校郵件管理者或資安人員。
- 如果已經輸入了帳號及密碼，請盡快至學校修改密碼之網頁，修改密碼。
- 定期更新主機防毒軟體及全機掃描。

出處:北區ASOC整理

加密貨幣挖礦
(PUA-OTHER Cryptocurrency Miner outbound connection attempt)

北區ASOC轄下學校11月事件第一名為加密貨幣挖礦，其規則名稱為 PUA-OTHER Cryptocurrency Miner outbound connection attempt，經過查詢大部分封包皆為門羅幣的挖礦事件。



	Tcp.stream	Udp.stream	Source	Src port	Destination	Dest port	Protocol	Length	Info
1-04 02:27:38.765642	0		140.	54556	149.28.199.108	443	TCP	263	54556 → 443 [PSH, ACK] Seq=1
1-04 02:27:43.561690	1		140.	42089	139.99.9.133	3333	TCP	294	42089 → 3333 [PSH, ACK] Seq=1
1-04 02:29:12.427603	2		140.	42095	139.99.9.133	3333	TCP	294	42095 → 3333 [PSH, ACK] Seq=1
1-04 02:31:45.924572	3		140.	42105	139.99.9.133	3333	TCP	294	42105 → 3333 [PSH, ACK] Seq=1
1-04 02:32:55.623974	4		140.	42111	139.99.9.133	3333	TCP	294	42111 → 3333 [PSH, ACK] Seq=1
1-04 02:34:36.545383	5		140.	42118	139.99.9.133	3333	TCP	294	42118 → 3333 [PSH, ACK] Seq=1
1-04 02:34:41.243801	6		140.	51063	149.28.199.108	443	TCP	263	51063 → 443 [PSH, ACK] Seq=1
1-04 02:35:58.418537	7		140.	42124	139.99.9.133	3333	TCP	294	42124 → 3333 [PSH, ACK] Seq=1
1-04 02:37:33.284895	8		140.	42131	139.99.9.133	3333	TCP	294	42131 → 3333 [PSH, ACK] Seq=1
1-04 02:39:01.163234	9		140.	42137	139.99.9.133	3333	TCP	294	42137 → 3333 [PSH, ACK] Seq=1
1-04 02:39:56.748733	10		140.	51074	149.28.199.108	443	TCP	263	51074 → 443 [PSH, ACK] Seq=1
1-04 02:40:09.829213	11		140.	42143	139.99.9.133	3333	TCP	294	42143 → 3333 [PSH, ACK] Seq=1
1-04 02:41:15.465291	12		140.	42148	139.99.9.133	3333	TCP	294	42148 → 3333 [PSH, ACK] Seq=1

Wireshark · Follow TCP Stream (tcp.stream eq 38) · request_1541987994.pcap

```
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"","pass":"","agent":"/ (Windows NT 6.1; Win64; x64) libuv/1.23.0 msvc/2017","algo":["cn","cn/2","cn/1","cn/0","cn/xtl","cn/msr","cn/xao","cn/rto"]}}
```

出處:北區ASOC整理

加密貨幣挖礦
(PUA-OTHER Cryptocurrency Miner outbound connection attempt)

經分析之後，可以發現此 IP 為 coinhive 挖礦程式的 domian。

Passive DNS Replication ⓘ

a.deepsecu.com

Date resolved	IP address
2018-11-05	149.28.199.108

Passive DNS Replication ⓘ

p.deepsecu.com

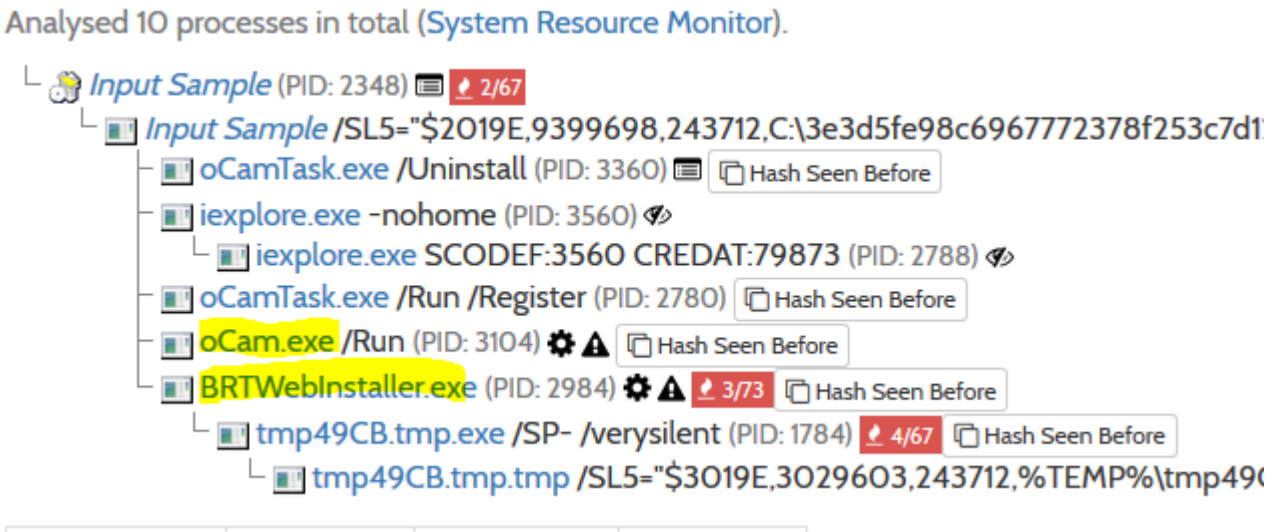
Date resolved	IP address
2018-10-31	172.104.188.159
2018-06-19	163.44.149.205
2018-06-08	118.27.7.221

出處:北區ASOC整理

加密貨幣挖礦

(PUA-OTHER Cryptocurrency Miner outbound connection attempt)

深入研究封包特徵後，可以發現依然與 oCam 錄影程式相關，其挖礦贊助軟體BRT.exe。



出處:北區ASOC整理

小結

1. 本事件與今年5月份的 OHSOFT mining 事件相同，皆為oCam BRT挖礦程式。

2. oCam 挖礦事件的中繼站的連線， 係以 DNS domain 查詢 IP，其IP會一直更換，單純阻擋 IP 成效並不好，建議阻擋 DNS domain name。

建議阻擋的 DNS domain name：

a.deepsecu.com
g.deepsecu.com
p.deepsecu.com
www.deepsecu.com

3. 目前IPS 針對挖礦事件，皆提供不少的阻擋規則。

勒索恐嚇郵件攻擊

北區ASOC轄下學校接獲勒索郵件攻擊，有使用者收到有駭客表示入侵其email帳戶及主機並要求支付800多美元的比特幣之勒索恐嚇信。

經查與TWCERT/CC發布的資安威脅案例類似，如參考連結：
https://m.facebook.com/story.php?story_fbid=2253444848218581&id=1670471206515951


前往首頁

台灣電腦網路危機處理暨協調中心 - TWCERT/CC

【資安威脅】本中心近期接獲通報，表示收到勒索恐嚇信件，本中心提醒此為詐騙信件請勿匯款
本中心近期接獲通報，表示收到有人掌握其硬碟檔案並要求於48小時內支付500美金之恐嚇信，經本中心查找與比對信件內容及比特幣錢包SiteKey等特徵，發現10月15日網路上亦有相同案例，如圖所示，認定為發信者未真正掌握受害人檔案系統之詐騙事件，提醒民眾勿匯款。
信件特徵：
1.信件開頭以"my nickname in darknet is XXXX", XXXX可能隨機更換。
2.信件內容表示對方已掌握帳戶密碼、瀏覽器歷史紀錄等資料，並取得您的所有通聯記錄、硬碟資料與照片。
3.要求48小時內支付500美元的比特幣至指定的帳戶。
TWCERT/CC提供以下防護建議：
1.密碼建議使用12個字元以上且英文、數字、符號混合。
2.應避免多個服務使用同一組密碼，以免遭到撞庫攻擊(說明如註解)。
3.收到電子郵件不任意開啟信件之附件或網路連結，以避免遭植入惡意程式竊取資訊。
4.確實持續更新電腦的作業系統、Office應用程式等至最新版本。
5.更新電腦防毒軟體病毒碼。
註解：什麼是撞庫攻擊?
人們與網路服務連結越來越深，各大網路都有帳號跟密碼資訊，但人們可能難以依據資安建議，一個服務用一個獨一的密碼，常是好幾個不同服務，所輸入的帳號密碼組合一樣，免得帳密常常忘記，得時常重設。人類的記性不足以及惰性，給予駭客可趁之機。只要取得某次服務帳密外洩的資料庫，賭一把看看其他服務是不是採用一樣的帳密，嘗試登入看看，不必用暴力破解法多次嘗試，就可合法登入受害者系統或服務。
參考連結：
[1]https://malwaretips.com/threads/email-received-from-supposed-darknet-hacker.87366/
[2]https://productforums.google.com/forum/#
[3]https://www.scamwarners.com/forum/viewtopic.php?f=9&p=374862

出處:北區ASOC整理

勒索恐嚇郵件攻擊

信件特徵

- 主旨為 **password (xxxxx) is compromised** 或 **Your password is xxxxx** 或 **your password xxxxx** 或 **password (xxxxx) for @mail.xxx.ntu.edu.tw is compromised**
- 信件內容表示已掌握使用者的郵件密碼、上網紀錄、通聯記錄、硬碟資料與照片，且已植入惡意程式。
- 要求支付**800**多美元的比特幣至指定帳戶。

出處:北區ASOC整理

勒索恐嚇郵件攻擊

建議防護措施

- 立即修改**email**密碼為強健密碼，**8**個字元以上英文**(**大小寫**)** 、數字、符號混用。不同服務使用不同帳密。
- 備份重要檔案。
- 謹慎防範釣魚信件攻擊 **(**參考**http://www.cc.ntu.edu.tw/mailtips/index.html)**
- 持續更新主機作業系統、**Office**應用程式及防毒軟體病毒碼。

出處:北區ASOC整理

大 綱

- 資安案例分享
  - ohSoft 軟體挖礦事件
  - CLDAP 反射式放大攻擊
  - 加密貨幣挖礦
  - 病毒式釣魚信件案例
  - 勒索恐嚇郵件攻擊
- **資通安全管理法**

資通安全管理法背景

- 資通安全管理法於107年6月6日總統令公布
- 107年11月21日發布資通安全管理法施行細則及管理辦法
- 行政院公告於108年1月1日全面施行

資通安全管理法重點

- 應符合資通安全責任等級分級辦法
- 應擬定與實作資通安全維護計畫
- 應擬定與實作資通安全事件通報及應變辦法
- 公務機關所屬人員資通安全事項獎懲

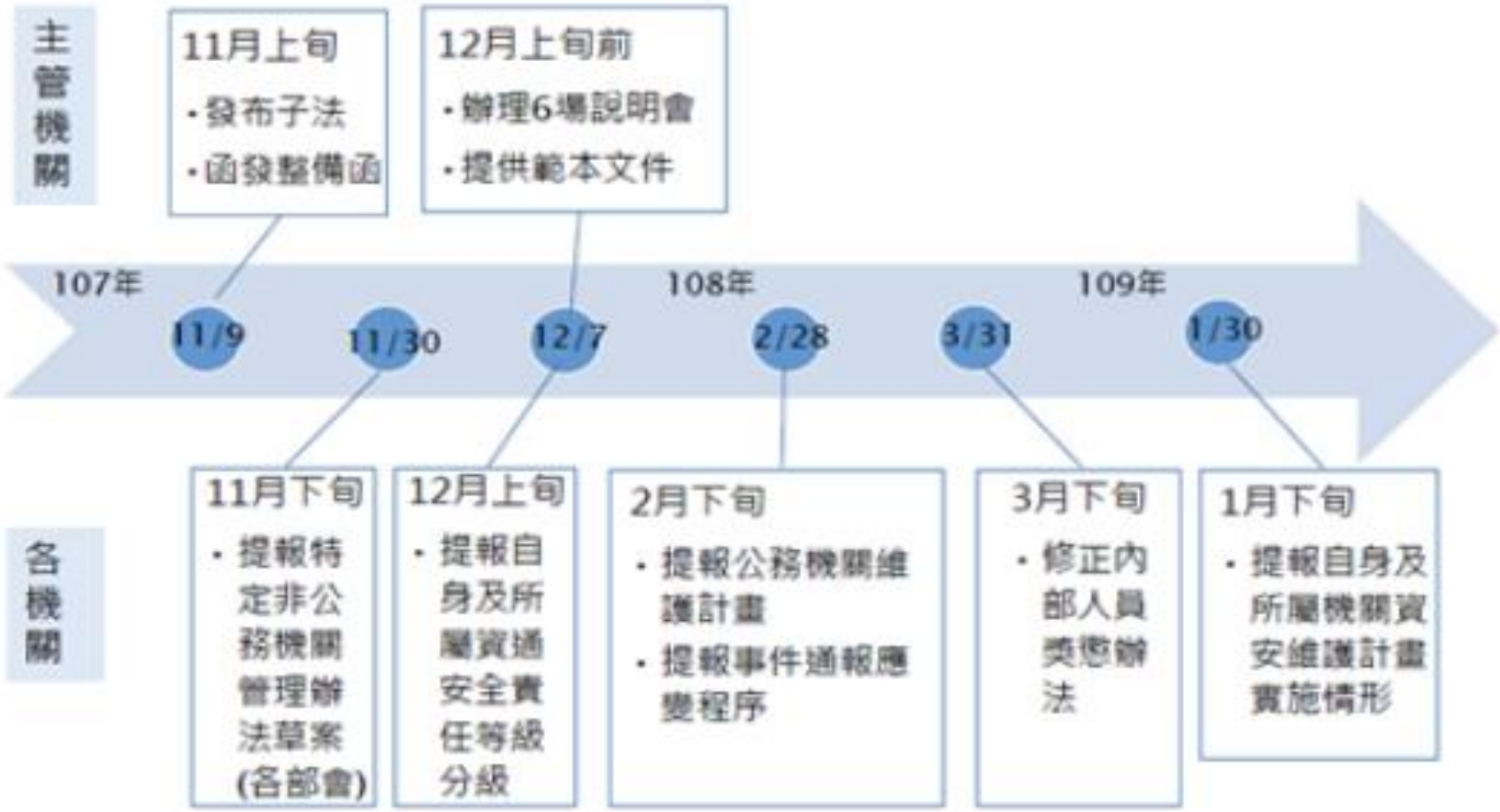
附表三 資通安全責任等級B級之公務機關應辦事項

制度面向	辦理項目	辦理項目細項	辦理內容
管理面	資通系統分級及防護基準		初次受核定或等級變更後之一年內依附表八完成資通系統分級，並完成附表九之控制措施。
	資訊安全管理系統之導入及通過公正第三方之驗證		初次受核定或等級變更後之二年內，全部核心資通系統導入 CNS 27001 資訊安全管理系統國家標準、其他具有同等或以上效果之系統或標準，或其他公務機關自行發展並經主管機關認可之標準，並於三年內完成公正第三方驗證。
	資通安全專責人員		初次受核定或等級變更後之一年內，配置二人；須以專職人員配置之。
	內部資通安全稽核		每年辦理一次。
	業務持續運作演練		每二年辦理一次核心資通系統持續運作演練。
	資安治理成熟度評估		每年辦理一次。
技術面	安全性檢測	網站安全弱點檢測	全部核心資通系統每年辦理一次。
		系統滲透測試	全部核心資通系統每二年辦理一次。
	資通安全健診	網路架構檢視	每二年辦理一次。
		網路惡意活動檢視	每二年辦理一次。
		使用者端電腦惡意活動檢視	每二年辦理一次。
		伺服器主機惡意活動檢視	每二年辦理一次。
		安全設定檢視	每二年辦理一次目錄伺服器設定及防火牆連線設定之檢視。
	資通安全監控管理機制		初次受核定或等級變更後之一年內，完成監控機制建置，並持續維運。
	政府組態基準		經初次受核定或等級變更後之一年內，依主管機關公告之項目，完成政府組態基準導入作業，並持續維運。
	資通安全防護	防毒軟體	初次受核定或等級變更後之一年內，完成各項資通安全防護措施之啟用，並持續使用及適時進行軟、硬體之必要更新或升級。
		網路防火牆	
		具有郵件伺服器者，應備電子郵件過濾機制	
		入侵偵測及防禦機制	
		具有對外服務之核心資通系	

資通安全管理法法近期工作事項

- 有關資通安全任等級規定公務機關B級單位，需配置兩位資通安全專職人員
- 108年1月31日前自訂”資通安全維護計畫”及”資通安全事件通報及應變程序”，並送教育部審查
- 108年3月31日前依「公務機關所屬人員資通安全事項獎懲辦法」規定修正內部平時考核規定

資通安全管理法重要時程



Q & A