資通安全通報演練

資訊中心 林皓儀

一、依據

1.行政院國家資通安全會報函頒之

「國家資通安全通報應變作業綱要」。

2.教育部函頒之

「教育部資通安全處理小組作業說明」。

二、目的

1.測試資安聯絡人聯絡管道是否暢通。

2.測試各單位於發現資安事件時，

是否可正確、快速執行通報作業。

三、演練工作內容

1.針對演練模擬事件研擬應變處理作為。

2.填寫【資安事件處理暨回覆單】回覆應變處理作為。

四、攻擊事件類型

入侵攻擊事件(INT)及網頁攻擊事件(DEF)

模擬狀況編號	攻擊類型（事件類型）	攻擊子類型（事件子類型）	攻擊事件說明
1	DEF	網頁置換	單位網站首頁遭竄改
2	DEF	釣魚網站	單位內某網站被植入偽造認證網站(釣魚網站)
3	DEF	惡意網頁	單位內網站被植入惡意網頁
4	DEF	惡意留言	單位內網站討論區被灌入大量不當留言
5	DEF	個資外洩	單位內透過不同方式散播個人資料
6	INT	對外攻擊	單位內某電腦重複嘗試入侵他人系統
7	INT	散播惡意程式	單位內部電腦中毒並迅速感染其他電腦
8	INT	BOT	單位內電腦中毒成為BOTNET成員
9	INT	SPAM	單位內某電腦大量散佈電子郵件
10	INT	中繼站	單位內部電腦被植入惡意程式後形成BOT中繼站

五、演練內容

(演練事件單編號:DRILL-AISAC-1593)(告���通報)網頁置換事件簡訊

寄件人： TACERT

收件人: service@cert.tanet.edu.tw

教育機構資安通報演練平台

演練事件類型:網頁置換事件簡訊

演練事件單編號:DRILL-AISAC-1593

原發布編號	DRILL-AISAC-1593	原發布時間	2016-12-12 10:16:51
事件類型	釣魚網站	原發現時間	2016-12-12 10:16:50
事件主旨	資安事件通告一貴單位[私立長庚大學]遭檢舉IP[XXX.XXX.XXX.XXX]有釣魚網頁		
事件描述	1. 貴單位遭檢舉網站有釣魚(Phishing)網頁，釣魚網頁位址如下：http://XXX.YYY.ZZZ/index.html 2. 教育部電算中心目前已經限制該IP對學術網路外的連線 3. 釣魚網頁指駭客使用與原版網頁一模一樣的盜版頁面（但URL不同）來誘騙使用者上當，在該頁面輸入個人資料，或是銀行帳號密碼，或是信用卡資料等。 4. 因多數釣魚網頁涉及金錢損失，嚴重性極大，請貴單位依照標準作業程序於規範時限內進行回報		
手法研判	無		
建議措施	一般來說，網頁被置換，表示主機被入侵或遭惡意程式感染，有可能是登入的帳號密碼被破解，或是使用者不小心下載惡意程式。若是是遭到入侵，入侵者通常會留下其他的後門，或者會修改您系統其他的設定檔，造成其他的損害。所以我們建議您： 一、如果該台主機是使用中的網頁伺服器： (1)找出被置換或被新增的頁面，刪掉它們。如果有可以用的主機備份，建議直接使用備份取代現有網頁檔案 (2)查看哪些不使用的埠號被打開了，找出那些埠號被什麼程式使用，如果是沒見過的程式，請找出該程式的路徑，並刪除相關檔案，並且關閉不使用的埠號。並在之後的幾天持續觀察該埠號是否又有活動，若是又有活動進行，建議您重灌整台主機，更新至最新後，更改慣用的登入帳號密碼。 (3)如果無法重灌，在刪掉被置換或是被新增的網頁之後，更新OS及service的patch，以及變更登入主機的帳號密碼，刪除不使用的使用者帳戶，關閉不使用的埠號以及服務 (4)沒有防火牆的主機務必安裝防火牆 (5)定期檢查system log或web server log查看是否有不明活動。 二、如果該主機僅是一般使用者的工作機，建議您直接備份需要的資料之後，重灌該台主機（若原本的主機OS過於老舊，請升級OS），並在安裝之後更新。		
此事件為演練事件，需要進行通報，請 貴單位資安聯絡人登入資安通報應變演練平台進行通報應變作業			
如果您對此通告的內容有疑問或有關於此事件的建議，歡迎與我們連絡。			

教育機構資安通報應變小組
演練網址：https://drill.cert.tanet.edu.tw/
專線電話：07-5250211
網路電話：98400000
E-Mail：service@cert.tanet.edu.tw

六、演練回覆說明

1.確認資訊安全事件弱點是否完全根除，
　若無法根除，填寫無法根除之理由。
2.應變及處置措施可參考建議處理方式填寫。
3.檢討暨改善可依單位實際情形填寫。
4.主管核簽後回擲資訊中心存檔備查，
　即完成資通安全通報演練。

Thank You

感謝聆聽