◎第一線人員	
機關名稱	花蓮縣秀林鄉水源國民小學
資安聯絡人	王永誠
EMAIL	s8622006@gmail.com
聯絡電話	03-857-0781
分機	12

◎區縣市網人員	
機關名稱	花蓮縣教育網路中心
資安聯絡人	陳毓倫

聯絡電話	03-846-2860#509
E-mail	allen@hlc.edu.tw

詳細資料			
發佈編號	DRILL-DEF-2019-1822	發佈時間	2019-09-18 10:52:19
事件類型	惡意網頁	發現時間	2019-09-18 10:52:19
事件主旨	資安事件通告–貴單位[花蓮縣秀林鄉水源國民小學]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		
處	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		

理建議	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。
參考資料	檢查埠號及其對應的網路活動可以在命令提示字元使用[netstat -anob]指令，或是使用微軟的免費小程式[TCPView]

1. 通報型態：	
告知通報編號：	DRILL-DEF-2019-1822
2. 事件發生時間：	2019-09-18 10:52:19
3. 確認為資安事件時間：	

4. 設備資料：	
ＩＰ位置：	210.240.49.229
網際網路位置：	http://www.syps.hlc.edu.tw/
設備廠牌、機型：	Acer AT110 F1
作業系統：	Windows XP SP2
受駭應用軟體：	sendmail server
已裝置之安全防護軟體：	
	防毒軟體： Avira 10.0.0.561 防火牆：iptables IPS/IDS：snort 2.8.3 其它：無
5. 資通安全事件：基本資料	
事件分類：	DEF-惡意網頁-
破壞程度：	學校網頁遭惡意置換為不明網頁,恐有帳號被盜問題
事件說明：	今日上午 10:5 學校網頁遭惡意置換為不明網頁,配合學務組辦理惡意頁移除,資安人員立即調高防火等級
6. 資通安全事件：影響等級及說明	
資安事件判斷：	
(1) 機密性衝擊 -1 級-非核心業務資訊遭輕微洩漏	

(2) 完整性衝擊 -1 級-非核心業務資訊或非核心資通系統遭輕微竄改
(3) 可用性衝擊- 1 級-非核心業務之運作受影響或停頓，於可容忍中斷時間內回復正常運作，造成機關日常作業影響
資安事件綜合評估等級：1 級
可能影響範圍 及損失評估
網頁連結錯誤,教學使用不便,影響課程,甚至可能同仁帳號被盜用,立即通報並處理完畢
7. 是否需要支援? 否
8. 通報完成時間： 2019-09-18 12:39:16
9. 通報事件單編號： 1822

◎緊急應變措施：
已停止伺服器之服務，待處理完成後再上線
解決辦法：
移除惡意不明網頁,回復超連結,增強防火牆層級
解決時間： 2019-09-18 12:39:10
◎改善措施：

改善辦法：

改善時間：

◎區縣市網通報審核

通報審核結果:通過

區縣市網審核時間:2019-09-18 13:48:53

◎區縣市網應變審核

區縣市網應變審核結果:無需審核

區縣市網應變審核時間:

◎資安通報應變小組通報審核

資安通報應變小組審核結果:未審核

資安通報應變小組審核時間:

◎資安通報應變小組應變審核

資安通報應變小組應變審核結果:無需審核

資安通報應變小組應變審核時間: