111 年 12 月 20 日基隆市教網中心 Botnet 攻擊事件處理時間表

日期	處理進度
111/12/20	發生網路連線無預警瞬斷，造成全市網路無法正常運作，立即因應召集教網中心機房防火牆及 coreswitch 的廠商調查發生原因。
111/12/21	發現全市連線(Session)數不正常，從平常每秒 25 萬筆爆增到每秒 800 萬筆，再深入調查發現是 BotNet（殭屍網路）攻擊，立即將外部 1600 多個 Botnet.CNC 黑名單的 IP 進行封鎖，封鎖後攻擊並無下降。
111/12/22	先行手動封鎖 35 個內部學校 IP。
111/12/23	發現市內攻擊擴散到 496 個 IP，再進行人工封鎖阻擋，並於處務公告 1776 通知各校因應。
111/12/25	狀況仍未改善，災情擴散已無法以人工方式阻擋，並可能造成防火牆崩潰全市所有學校斷網，在與原廠工程師緊急開會決議，以下列兩條件設立自動封鎖規則阻擋災情擴大。 • 確定受到感染(Botnet.CNC)。 • Session 數超過 2,000 筆/每秒(PC 正常值約為 200 筆/每秒.單一網頁約 40-60 筆/每秒)，開啟自動封鎖。
111/12/26	成功阻止殭屍網路擴散，網路連線恢復平常每秒 25 萬筆，故上簽教育處長官通報本市事件處理，並於 19：00 將原本封鎖歸零，**之後有感染行為才加入封鎖清單。**
111/12/27	處務公告 1788 公告本市各校公告本市各校後續因應作為。
112/1/7	目前封鎖外部 1730 個 IP，內部封鎖 145 個 IP ，網路正常運作中。