博幼基金會資安事件報告

日期：2026.11.09

事件發生_確認駭客入侵系統

- 115/10/9 02:10 本會 國尊Cyberhood 主機（ECP）遭駭客入侵駭客利用系統漏洞植入後門程式。
- 115/10/9 03:39 駭客篩選含信用卡卡號、到期日之資料，下載約 15,000 筆。
- 115/10/9 04:38 兩個資料庫遭下載；設定檔、SSL 憑證私鑰、系統帳號密碼雜湊亦遭讀取。
- 115/10/10 16:38，駭客冒用本會信箱 service@ecp.boyo.org.tw 寄出 2,796 封假冒郵件(發送「捐款成功通知」或「定期定額捐款暫停」等釣魚信件)

事件發生時本會應變措施

- 115/10/10 17:00 接獲捐款人通報，本會隨即阻擋發信並封鎖後門、斷網隔離受駭主機。立即於本會官網、Facebook、LINE@ 等數位管道公告提醒防詐訊息。
- 115/10/10 19:41 暫停線上捐款平台
- 115/10/10 22:00 至警局報案，10/11 00:01完成報案
- 115/10/11 09:07 國尊科技公司接獲本會通知，啟動應變
- 115/10/11 本會通報主管機關衛生福利部
- 115/10/11-10/19 本會以簡訊、市話語音、Email 與紙本信件通知捐款人，共 20.6 萬次。
- 115/10/12 暫停10月份定期定額扣款，避免捐款人混淆。
- 115/10/14 向調查局提出刑事告訴狀；10/15 調查局派員至本會實地調查與蒐證；10/27 調查局立案。

事件發生後的系統緊急防護措施

- 115/10/12 上午以原始 ISO 檔重建新主機，覆蓋漏洞修補程式並調整權限。
- 新主機暫時只於內網開放，防火牆依漏洞設定黑名單。
- 封鎖攻擊來源 IP：50.7.252.187–189、134.195.100.26、63.140.1.233。
- 全面變更資料庫密碼，並更新憑證。

事件發生後系統改善措施

- 定期更新各項系統服務版本，留意資安漏洞資訊。
- root 密碼加強控管，降低外流機率。
- 調整 ECP 主機網路架構，確保主機位於本會防火牆有效保護範圍內，並落實網路存取權限控管及日誌集中管理，以降低外部入侵風險，提升資安事件偵測與追蹤能力。
- 建立寄信異常即時告警機制。
- 建立登入、流量異常告警機制，定期檢測。
- 委請專業資安公司 MDR 全天候監控，115/10/13–11/3 無資安事件。
- 第三方檢測：鑒真數位有限公司 115/11/4 針對網頁弱點掃描，高、中風險 0 項，2 項低風險已於 115/11/5 修補。

事件發生後系統改善措施

- 與國尊研擬個資資安增補協議：漏洞修補、事件通報、遠端存取與稽核。
- 建立廠商維護紀錄制度，每次維護留存紀錄供查核。
- 未來系統架構將升級為分散式架構，後端資料庫隔離並加密。
- 持續委請專業資安公司 MDR 全天候監控。

結語

感謝第一時間通報我們的捐款人，也向受到驚擾的每一位支持者致上最深的歉意。系統已重建並通過第三方檢測。本會將持續全天候監控，以最高標準守護每一份信任，也期盼與捐款人、合作夥伴及社會各界攜手，持續為偏鄉孩子的學習努力。

- **防詐四原則：**勿點不明連結、認明官方 LINE 認證盾牌、切勿提供個資、切勿操作 ATM 或網銀
- **聯繫方式：**博幼總會服務電話 (049) 291-5055　|　官方 LINE @boyo