張貼日期：2025/02/11

【攻擊預警】近期勒索軟體攻擊頻繁，請各單位加強防範。

- 主旨說明:【攻擊預警】近期勒索軟體攻擊頻繁，請各單位加強防範。
- 內容說明:
  - 近期發生學校與醫院遭受勒索軟體攻擊之事件，駭客透過系統管理者電腦進行橫向攻擊。再利用網內其他主機散播勒索軟體加密檔案，導致多主機內的服務中斷與資料被加密。另在醫院受到勒索軟體Crazy Hunter之攻擊，目前已知有下列惡意程式名稱:bb.exe、crazyhunter.exe、crazyhunter.sys、zam64.sys、go3.exe與go.exe、提供參考。
  - 面對勒索軟體攻擊，事先預防勝於事後應變，建議各單位除加強資料備份外，亦可建立離線備份，對於單位內各伺服器之安全性也應定期檢視，相關作業系統及自動備份系統安全性更新亦需留意。
  - 在帳號與密碼之安全建議，除定期更換密碼與加強密碼強度外，應避免同一管理者使用同一組密碼同時管理多台伺服器之情形。
- 影響平台：全
- 建議措施:
  1. 定期進行系統與防毒軟體的安全性更新，如無法更新應佈署對應的防護措施。
  2. 建議留意可疑電子郵件，注意郵件來源正確性，勿開啟不明來源之郵件與相關附檔。可掃描郵件及附檔，以偵測和阻擋惡意程式入侵。例如:開啟檔案前可使用防毒軟體掃描郵件附檔，並確認附檔檔案類型，若發現檔案名稱中存在異常字元(如exe.pdf, exe.doc, pdf.zip, lnk, rcs, exe, moc等可執行檔案附檔名的逆排序)，請提高警覺。
  3. 可落實網段切割隔離機制，縮小可能被攻擊的主機數量。
  4. 強化高權限帳戶的監控措施，如登入次數過多則關閉該帳戶、紀錄登入行為、偵測可疑行為等。
  5. 採用多因子身分認證機制。
  6. 定期進行檔案備份，並遵守備份 321 原則 ：
     1. 資料至少備份 3 份
     2. 使用 2 種以上不同的備份媒介
     3. 其中 1 份備份要存放異地 。
  7. 對於重要核心系統主機可安裝EDR (Endpoint Detection and Response)端點偵測與回應的技術服務，可偵測並調查主機和端點上的可疑活動，以期阻擋勒索軟體攻擊。

計算機與通訊中心
網路系統組 敬啟