

# 覆 醫師公會全國聯合會

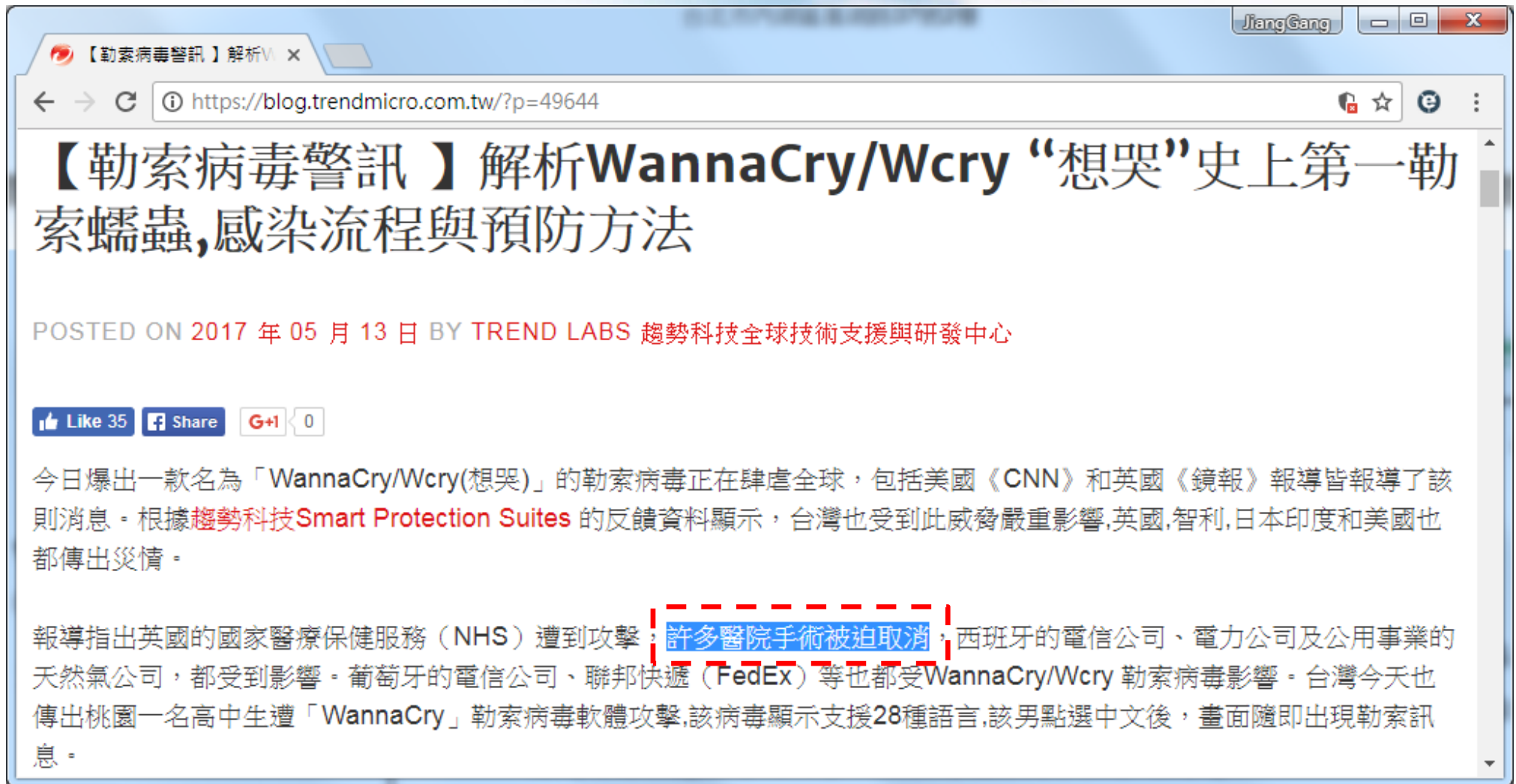
## 遭遇類似Wannacry勒索病毒攻擊之防護方案

中華電信數據分公司  
7/11/2017



*Refresh your life*



# WannCry勒索病毒危害嚴重

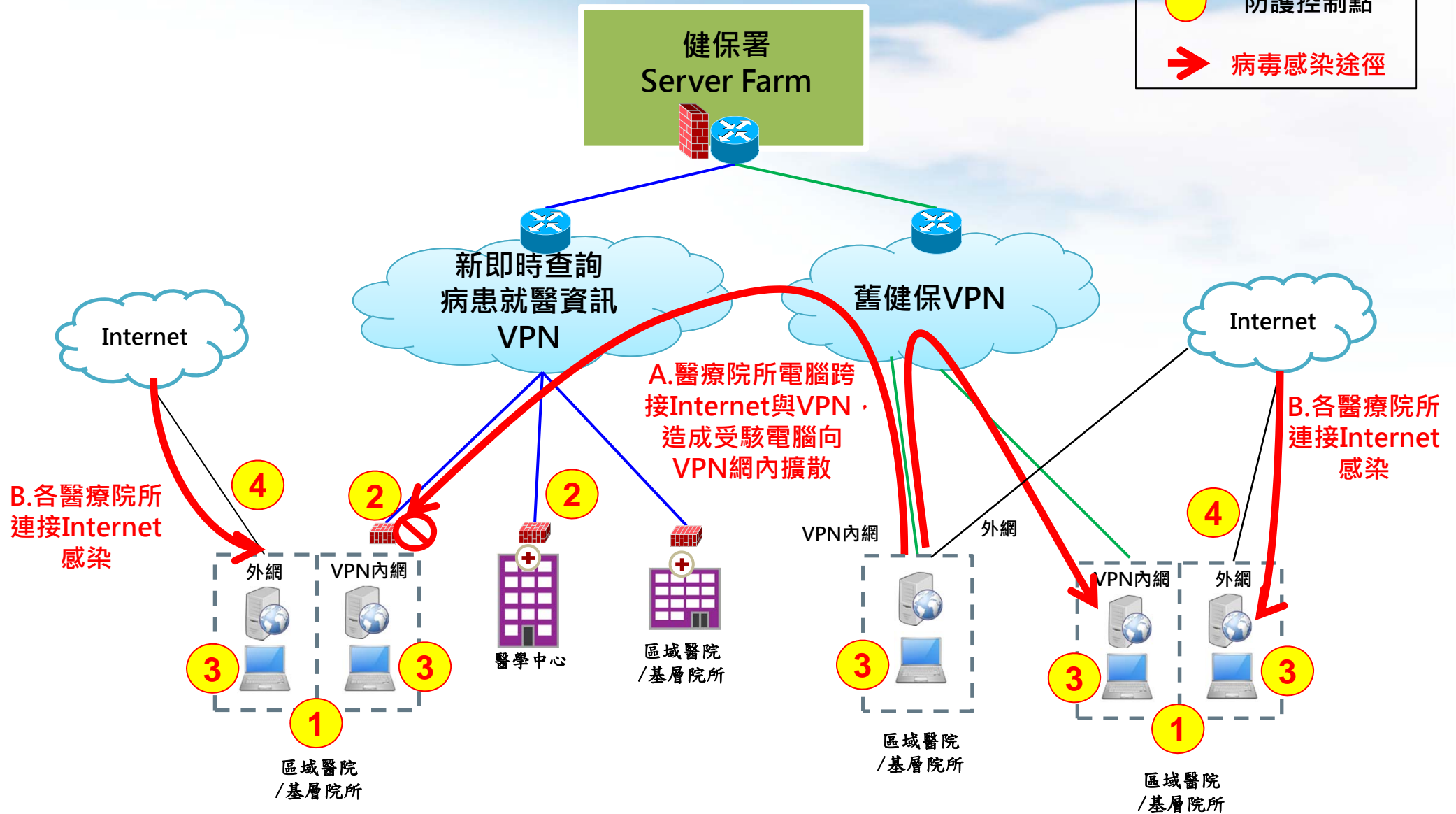


The screenshot shows a web browser window with the address bar displaying <https://blog.trendmicro.com.tw/?p=49644>. The page title is **【勒索病毒警訊】解析WannaCry/Wcry “想哭”史上第一勒索蠕蟲,感染流程與預防方法**. The post is dated **2017年05月13日** and attributed to **TREND LABS 趨勢科技全球技術支援與研發中心**. It features social media sharing buttons for Like (35), Share, and G+ (0). The main text reports that the Wannacry/Wcry ransomware is spreading globally, affecting major news outlets like CNN and the BBC, as well as various countries including Taiwan, the UK, Chile, India, and the US. A specific detail is highlighted with a red dashed box: **許多醫院手術被迫取消**. Other affected entities mentioned include the NHS in the UK, Spanish telecom and utility companies, Portuguese telecom, and FedEx. A case in Taiwan is also noted, where a high school student's computer was attacked, displaying a ransom message in Chinese.




# 健保VPN示意圖

圖例說明:

-  防護控制點
-  病毒感染途徑



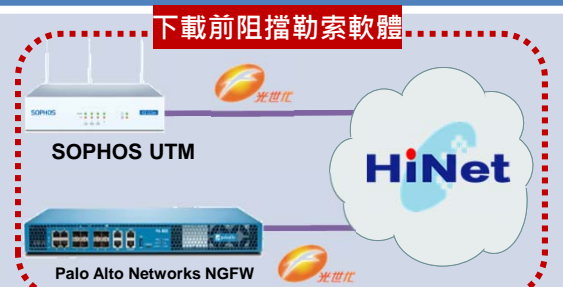


# 各醫療院所防護建議

感染途徑	控制點	防護建議	中華電信防護產品
A. 醫療院所 電腦跨接 Internet 與VPN， 造成受駭 電腦向 VPN網內 擴散	1	<b>確保健保醫療網VPN內網封閉性</b> ✓ 為保持網路安全性，建議醫療院所不應將VPN內之主機跨接Internet	
	2	<b>建議各醫療院所移轉至新健保醫療網</b> ✓ 因前端有防護設備，當事件爆發，可緊急設定防護規則阻擋病毒擴散	
	3	<b>終端主機作業系統與防毒軟體應確保為最新版本</b> ✓ 終端應避免使用EOF之作業系統，例如：Windows XP與Windows 2003 server，並定期更新作業系統以及防毒軟體 ✓ 中華電信企業版端點防護可協助阻擋勒索病毒攻擊 <b>重要伺服器或主機應定期執行離線備份</b> ✓ 可透過離線備份或商用資料保護方案 ✓ 中華電信企業版檔案安心存資安產品可有效保護重要資料	<div style="border: 2px dashed orange; padding: 10px; margin-bottom: 10px;"> <p style="text-align: center; background-color: orange; color: white; margin: 0;">執行前阻擋勒索軟體</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p><b>SOPHOS</b>新世代端點防護軟體 InterceptX</p> </div> <div style="text-align: center;">  <p><b>PAN</b> 新世代端點 防護軟體 TRAPS</p> </div> </div> </div> <div style="border: 2px dashed green; padding: 10px;"> <p style="text-align: center; background-color: green; color: white; margin: 0;">加密前阻擋勒索軟體</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  </div> <div style="text-align: center;"> <p><b>SecureBox</b> 檔案安心存</p> </div> </div> </div>





# 各醫療院所防護建議

感染途徑	控制點	防護建議	中華電信防護產品
B. 各醫療院所連接Internet感染	4	<p><b>連接Internet出口佈署防火牆/IPS阻擋攻擊流量</b></p> <ul style="list-style-type: none"> <li>✓ 阻擋來自Internet的掃描攻擊</li> <li>✓ 中華電信資安艦隊UTM都可有效協助客戶端防護</li> </ul>	<p><b>下載前阻擋勒索軟體</b></p> 
	3	<p><b>終端主機作業系統與防毒軟體應確保為最新版本</b></p> <ul style="list-style-type: none"> <li>✓ 終端應避免使用EOF之作業系統，例如：Windows XP與Windows 2003 server，並定期更新作業系統以及防毒軟體</li> <li>✓ 中華電信企業版端點防護可協助阻擋勒索病毒攻擊</li> </ul> <p><b>重要伺服器或主機應定期執行離線備份</b></p> <ul style="list-style-type: none"> <li>✓ 可透過離線備份或商用資料保護方案</li> <li>✓ 中華電信企業版檔案安心存資安產品可有效保護重要資料</li> </ul>	<p><b>執行前阻擋勒索軟體</b></p>  <p><b>加密前阻擋勒索軟體</b></p> 



*Value Creator for  
Investors, Customers, Employees, and Society*

敬請指教!

