

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

【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

POSTED ON 2017 年 05 月 13 日 BY TREND LABS 趨勢科技全球技術支援與研發中心

Like 35 Share G+ 0

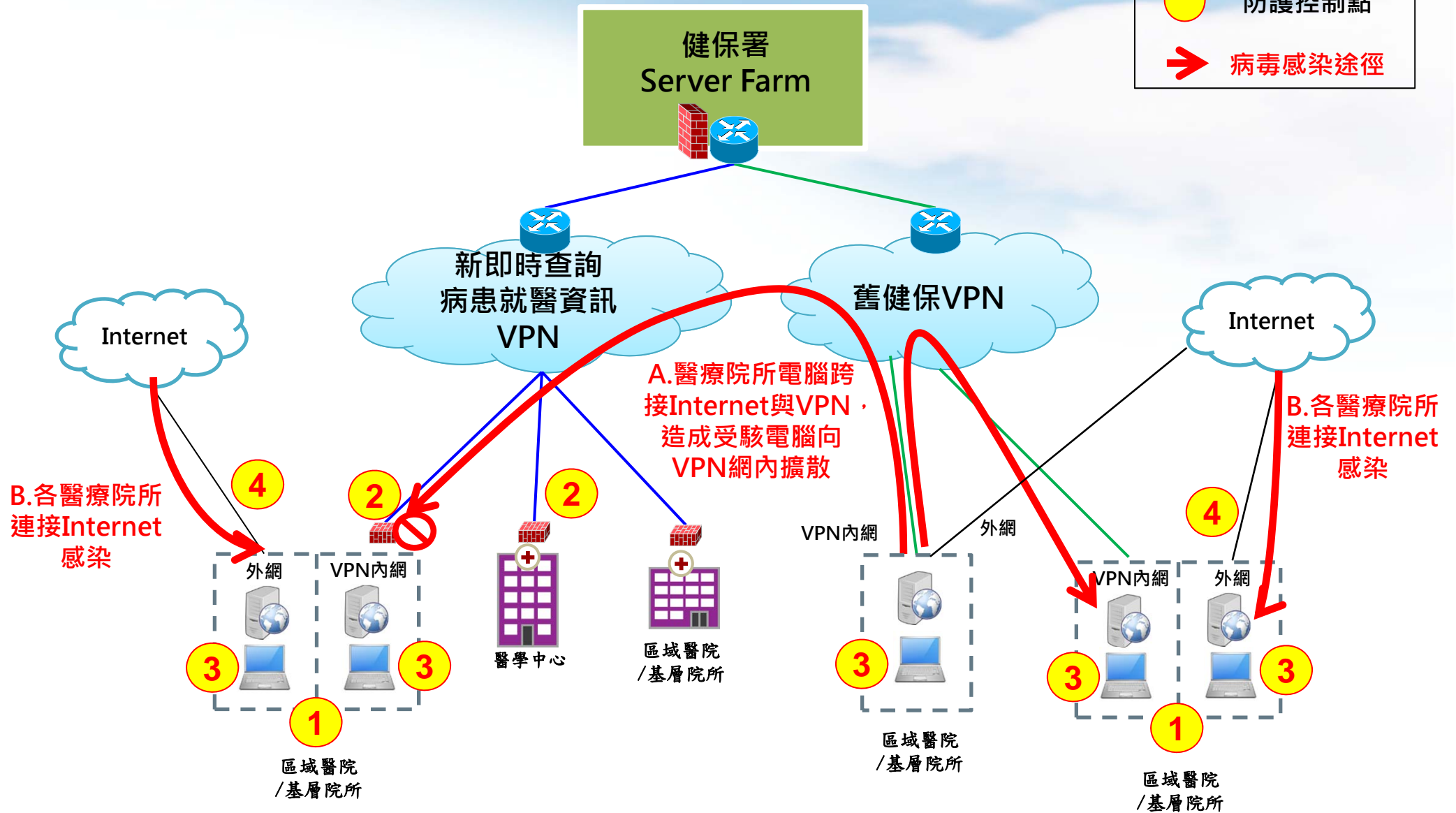
今日爆出一款名為「WannaCry/Wcry(想哭)」的勒索病毒正在肆虐全球，包括美國《CNN》和英國《鏡報》報導皆報導了該則消息。根據趨勢科技Smart Protection Suites的反饋資料顯示，台灣也受到此威脅嚴重影響，英國、智利、日本印度和美國也都傳出災情。

報導指出英國的國家醫療保健服務（NHS）遭到攻擊，許多醫院手術被迫取消，西班牙的電信公司、電力公司及公用事業的天然氣公司，都受到影響。葡萄牙的電信公司、聯邦快遞（FedEx）等也都受WannaCry/Wcry勒索病毒影響。台灣今天也傳出桃園一名高中生遭「WannaCry」勒索病毒軟體攻擊，該病毒顯示支援28種語言，該男點選中文後，畫面隨即出現勒索訊息。



健保VPN示意圖

圖例說明:

- 防護控制點
- ➔ 病毒感染途徑

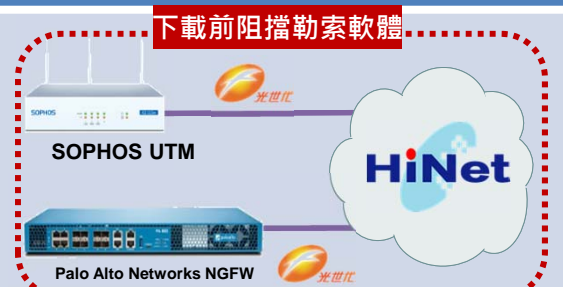




各醫療院所防護建議

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	確保健保醫療網VPN內網封閉性 ✓ 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	建議各醫療院所移轉至新健保醫療網 ✓ 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	終端主機作業系統與防毒軟體應確保為最新版本 ✓ 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 重要伺服器或主機應定期執行離線備份 ✓ 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	<p>執行前阻擋勒索軟體</p>  <p>SOPHOS新世代端點防護軟體 InterceptX PAN新世代端點防護軟體 TRAPS</p> <p>加密前阻擋勒索軟體</p>  <p>SecureBox 檔案安心存</p>



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>連接Internet出口佈署防火牆/IPS阻擋攻擊流量</p> <ul style="list-style-type: none"> ✓ 阻擋來自Internet的掃描攻擊 ✓ 中華電信資安艦隊UTM都可有效協助客戶端防護 	<p>下載前阻擋勒索軟體</p> 
	3	<p>終端主機作業系統與防毒軟體應確保為最新版本</p> <ul style="list-style-type: none"> ✓ 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 <p>重要伺服器或主機應定期執行離線備份</p> <ul style="list-style-type: none"> ✓ 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 	<p>執行前阻擋勒索軟體</p>  <p>加密前阻擋勒索軟體</p> 



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

敬請指教!

