留意新冠病毒以外的病毒

遠端工作的安全

近期2019冠狀病毒病(COVID-19)第五波大爆發，全港每天動輒上千確診，為免公司「冧檔」，不少公司已安排員工分組在家工作。現時遠端工作毫無難度，網絡上也有不少免費的遠端控制軟體供人使用，較知名的有TeamViewer、Chrome及AnyDesk。但知名不一定安全，越是知名的軟體越容易成為黑客目標，遠端桌面協定(Remote Desktop Protocol, RDP)亦成為近年勒索軟體感染的主要途徑。

不少人家中的電腦仍處於「裸奔」狀態，一直未有安裝合適的防毒軟件，又或者家中電腦有使用從網上下載的盜版軟件。這固然是一個極危險的安全漏洞，但就算是進行電腦遠程控制時，亦會令公司需要面對更高的網絡攻擊風險。而且你有想過家用的無線路由器也會被黑客利用漏洞取得攻擊碼嗎?

你家中的路由器安全嗎? 有適當的防護嗎?

家用路由器通常處於24小時開啟的狀態，一般使用者可能只會使用由網絡供應商提供的路由器，或者購買一些可以提供較快速度的路由器，但你有為你的路由器作定期檢查或進行韌體更新嗎?有妥善設定SSID和密碼嗎?

遠端桌面協定是內建在Windows作業系統的功能，可以讓用戶透過網路來連接另外一台電腦。RDP常會被針對性攻擊/鎖定目標攻擊來取回竊取資料，黑客會利用網路設備所存在的漏洞，修改路由器的設置，對你的網路進行監控，或是取得IoT#裝置的控制權，從監視攝影機等網路通訊設備，任意窺探用戶私隱，竊取資料等。

#物聯網(IoT)是指連結到互聯網的設備網絡，可以記錄或接收數據

竊來的資料會放到網路市場出售，還可以將監控的系統植入惡意程式，將無線路由器等IoT連網設備變成殭屍網路的幫兇，再利用它們對特定對象發動大規模DDoS攻擊。此外，針對RDP展開攻擊並不需要與用戶互動，因而令其更難被偵測。

防毒軟件是電腦最基本的防禦系統配備，它會協助用戶監控電腦程式的一舉一動，掃瞄系統是否含有病毒等惡意程式，另外安裝防毒軟件亦可增加黑客破解的困難度，可以在一定程度上保護電腦免受一般的黑客攻擊。

無線網路安全事項:

1. 修改路由器出廠預設的網路名稱
2. 將無線網路設定的加密方式設為WPA2##加密
3. 設定複雜而且強度較高的無線網路存取密碼
4. 修改後台管理介面密碼
5. 定期為無線網路設備進行維護更新，修補有漏洞的韌體
6. 另可參考eGarden於2021年2月發出的Guideline on Secure Remote Access Connection

歐盟網路安全局(ENISA)亦有為用戶提供一些建議，如果用戶想檢查自己的路由器設定有否被竄改，可使用F-Secure Router Checker。

為人為己，我們除了對不斷變種的2019冠狀病毒病(COVID-19)作出防禦外，自己家中的網絡安全亦要好好管理，避免因個人疏忽導致電腦病毒經由RDP攻擊公司網路。

F-Secure Router Checker

##WPA2是經由Wi-Fi聯盟驗證過的IEEE 802.11i標準的認證形式