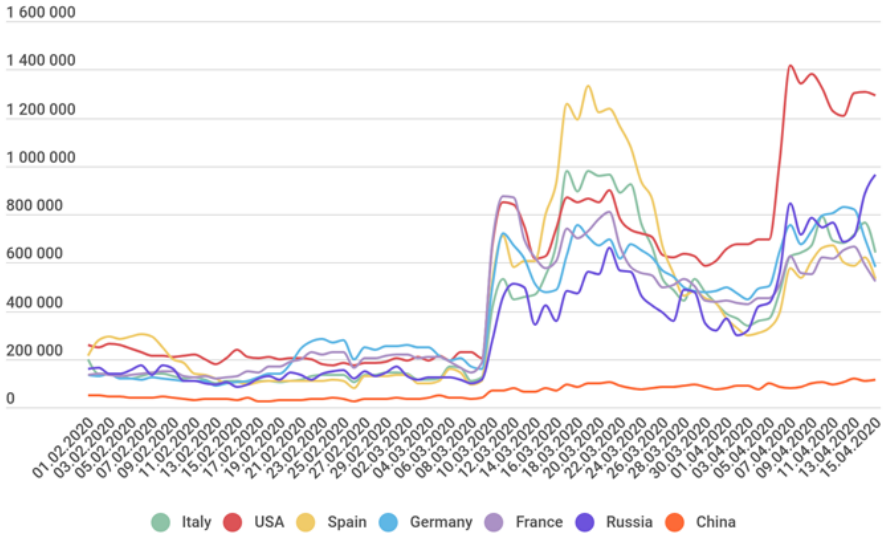
危機四伏的遠端桌面連線

ithome.com.tw/tech/137788



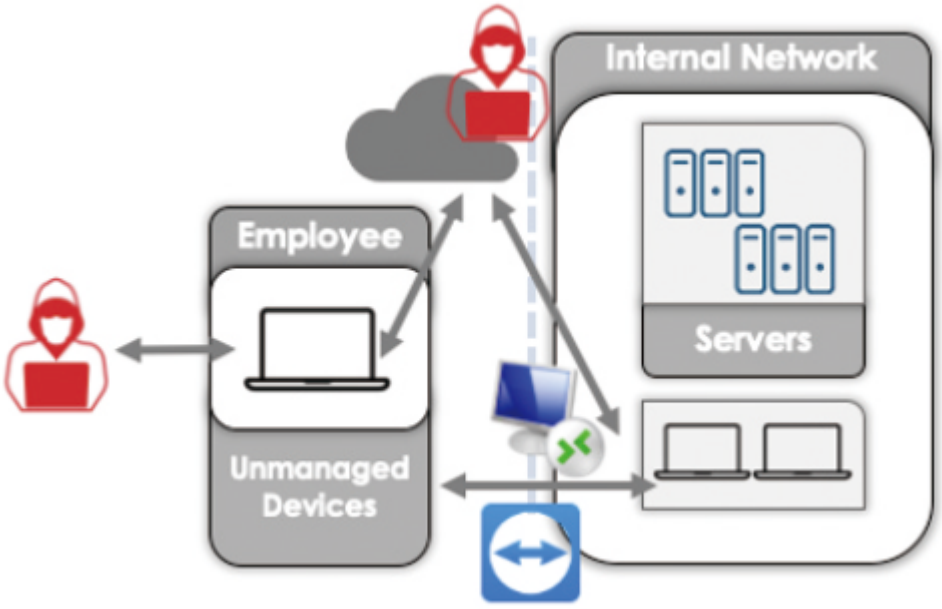
武漢肺炎全球確診人數直逼5百萬，許多企業、機構都採取部分或全員在家辦公的模式，也維持一段不算短的時間，然而，想長期實現這種作法，如何確保資安將是大考驗。

首先須讓員工能夠安全地透過網際網路連回公司，存取位於內部網路的資訊系統，以及各式資源，例如共用檔案與資料夾，而為了確保連線過程的機密性，企業需要開設VPN，並確保員工都能順利透過加密網路連線連回公司。

企業可能也會同時搭配雲端服務型態的多種網路應用解決方案，例如：即時通訊、電子郵件、網路硬碟／檔案共享與同步、視訊會議，來因應多人協作。

但上述方式並不一定適合每種工作情境，例如，員工存取一些公司應用系統時，需要基於辦公室個人電腦的既有環境設定才能連上，但家中電腦並未套用這些組態或缺乏系統必備的其他應用軟體，無法單靠使用者來操作相關設定；或是他們平時所儲存的檔案與資料夾，並未集中到公司設置的共用儲存區，而是放在辦公室的個人電腦當中。

為了能在短時間解決這樣的問題，目前有不少企業開放員工使用遠端桌面軟體（Remote Desktop）。目前這類產品的選擇很多，可採用Windows內建的遠端桌面連線，當中採用的是微軟發展的遠端桌面協定（RDP），或是開放原始碼軟體，例如，VNC（Virtual Network Computing），以及衍生的TightVNC、UltraVNC，此外，還有TeamViewer、Splashtop、Netop等商用軟體軟體，以及瀏覽器外掛Chrome Remote Desktop。



圖片來源／FireEye

若要讓在家的員工連上辦公室電腦，並維持相同作業方式，最簡單的作法，就是使用Windows內建的遠端桌面連線，或使用TeamViewer這類軟體。但在這樣直連的架構下，須注意電腦暴露在網際網路的程度，因為駭客可透過網路掃描，找到開放的網路埠，也能利用暴力破解、帳號填充等方式，強行登入。

遠端桌面連線大行其道，這類設備大量暴露，引起駭客覬覦

而在武漢肺炎爆發以後，VPN與遠端桌面的用量大增。根據網際網路連網設備搜尋引擎Shodan今年3月底的公告，執行VPN相關協定的伺服器從近750萬臺，在2月增加到近1千萬臺，提升幅度達到33％；而暴露在網際網路、採用遠端桌面協定的設備當中，若是使用預設3389埠的設備數量，這段期間增加41.5％，如果從RDP另一個常用的3388埠來看，這類設備數量成長36.8％。

Shodan認為，使用RDP設備在網際網路暴露的數量成長，可以解釋為許多組織正朝向遠端辦公的模式所致，因為RDP是Windows使用者遠端管理工作站或伺服器常用的方法，不過，長期以來，都有相關的資安問題和使用風險，因此，一般而言，不該在毫無防備的狀態下，開放公開存取。

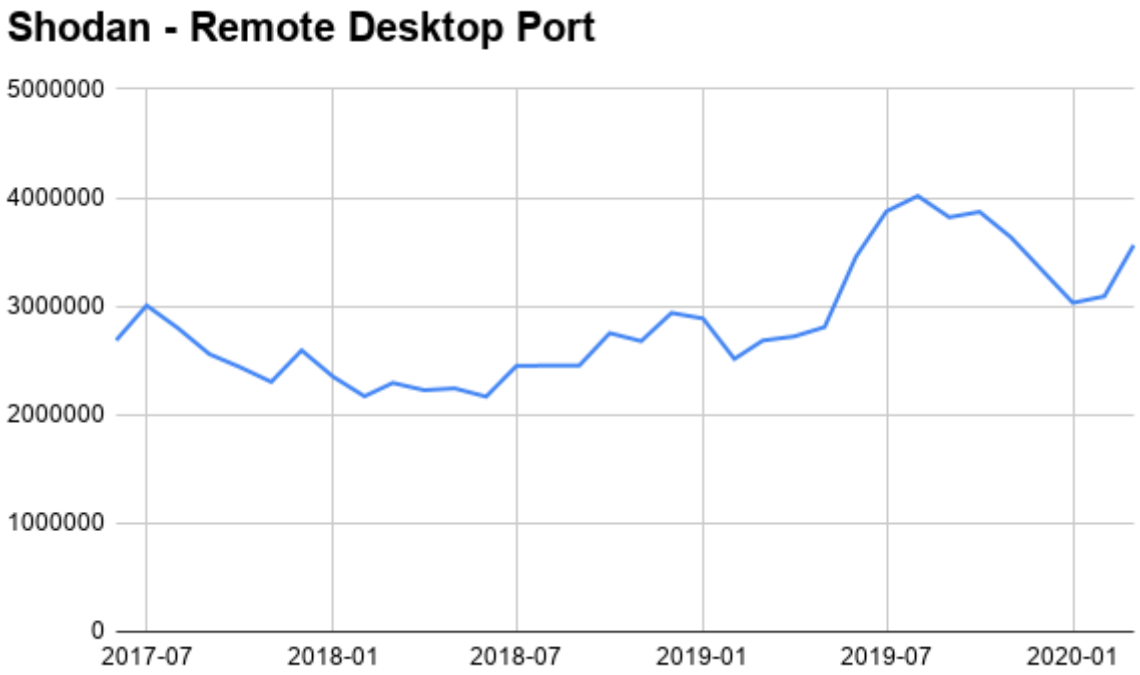
另一家主打外部攻擊面管理應用的資安廠商Reposify，也在此時提出更驚人的數據，根據他們的偵測，3月暴露在網際網路的RDP設備數量超過470萬個，它們正面臨潛在的攻擊風險，相較於1月，增加了127％。若從這些設備的IP位址來看，Reposify表示，大部分來自雲端、虛擬或實體代管業者，使用者從這些地方連至Windows電腦。

而這樣的現象也類似Shodan的分析結果——暴露在網際網路的RDP設備，已超過4百萬臺；從5大來源來看，有4家是雲端服務業者，1家是電信業者。

即便如此，或許有人仍會認為，使用RDP的設備暴露在網際網路上，只是存在著受到攻擊的風險，不等於已成為攻擊目標，以及正在面臨攻擊。然而，近期，有幾家資安機構和廠商發現了一些跡象。

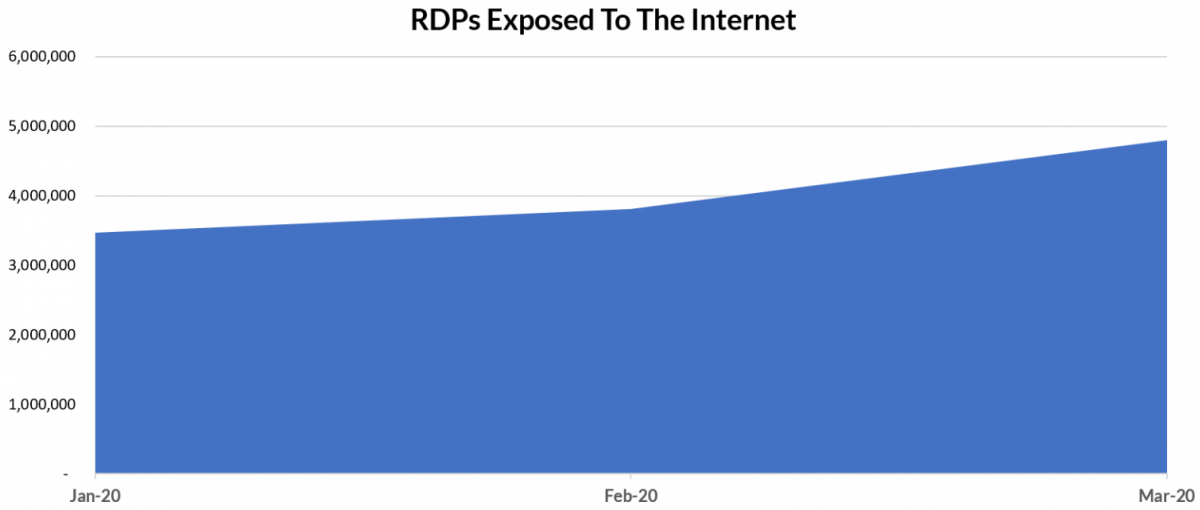
例如，在4月7日，美國系統與網路安全協會（SANS Institute）發布新聞稿，他們發現攻擊者對於RDP的興趣提升了30％，而這剛好與近期RDP設備暴露在網際網路數量大增的狀況，相互呼應。

SANS技術協會研究院大老Johannes Ullrich表示，他們觀察到攻擊者用於掃描網際網路RDP應用的IP位址數量，在3月增加了3成，平均每天有2,600到3,540個IP位址發動攻擊；此外，他們也發現攻擊者會主動購買這些RDP伺服器的帳號密碼，而一臺被滲透的RDP伺服器，之後往往又會導致整個系統完全被攻破，同時，也有可能用於攻擊或濫用位於內部網路的其他系統。



圖片來源／Shodan

企業大舉開放員工在家辦公，相對地，也促使特定網路服務的用量大增，根據網際網路連網設備搜尋引擎Shodan長期追蹤統計，今年第一季暴露在網際網路上的RDP設備，多達3百萬臺以上。



圖片來源／Reposify

資安廠商Reposify表示，暴露在網際網路的RDP設備已超過470萬臺。

RDP暴力破解攻擊大舉來襲

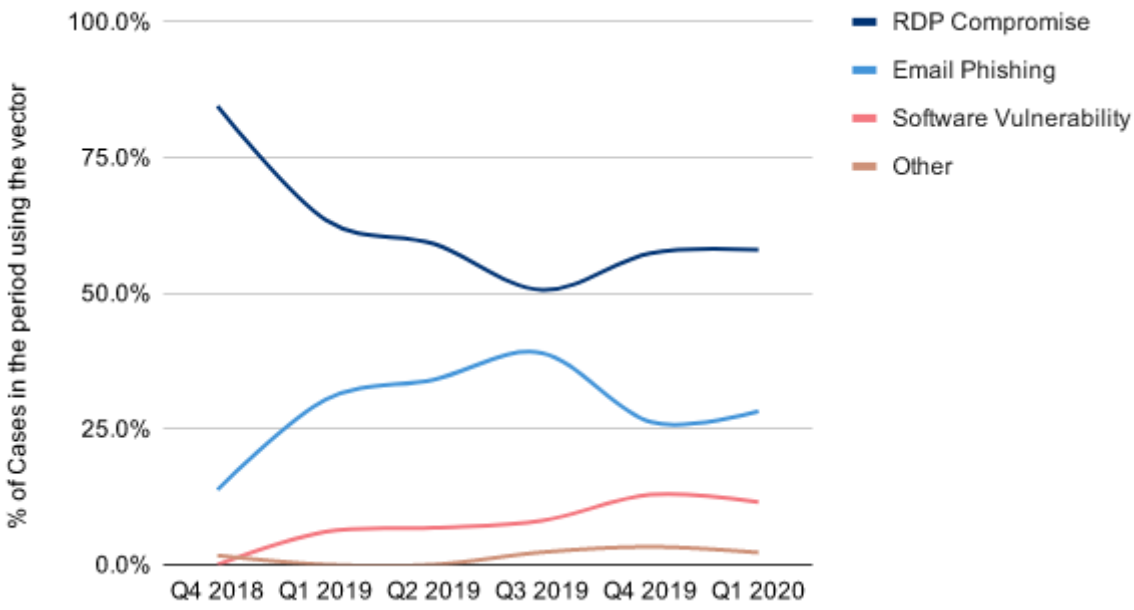
但實質的網路攻擊真的出現了嗎？根據資安廠商Kaspersky 4月底公布的觀察報告，針對RDP使用者帳號與密碼進行暴力破解的攻擊（brute-force attack），從3月開始暴增，而且，災情遍及全球。

該公司也清楚列出中、美、義、西、德、法、俄的攻擊走勢。根據他們的觀察，在1月2日到3月9日期間，7國面臨的RDP攻擊數量，都在20萬次以下（中國低於5萬次），但到了3月10日、11日，這些國家面臨的RDP攻擊次數全部急遽陡增，美、法兩國甚至都超過80萬次，之後各國還有第二波、第三波暴增的狀況。

何謂暴力破解攻擊？這是指攻擊者針對系統或服務的使用者登入機制，不斷嘗試各種帳號密碼，直到發現正確的組合為止，而這樣的身分比對搜尋，會基於隨機的字元、常用的字詞，或是被外洩的帳號密碼來進行。以RDP而言，一旦任何人成功找到可登入的帳密，就能和原本的合法使用者一樣，透過網路存取這臺開放RDP用途的電腦，進而胡作非為。

近幾年以來，RDP已成勒索軟體感染的主要路徑

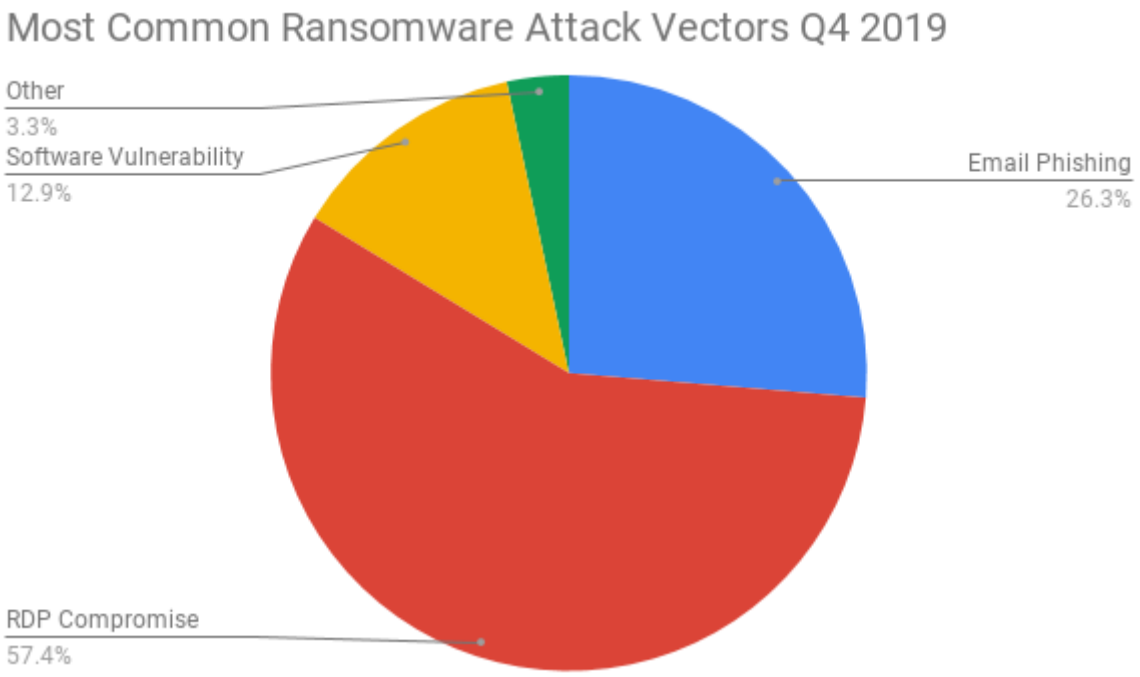
圖片來源／



Coveware

令人聞之色變的勒索軟體威脅，過去我們總認為主要是透過網路釣魚郵件與軟體安全性漏洞，來進行散播與滲透，但近年來，RDP也成為這類攻擊發動的主要管道。

另一個證據，是透過RDP存取的個人電腦，已成為當前勒索軟體攻擊最常見的攻擊路徑。例如，在4月底，專攻勒索軟體攻擊應變與分析的業者Coveware，他們的報告就特別提到這樣的狀況，近一年多以來，RDP洩漏被勒索軟體攻擊採用的比例，都維持在50％以上，自2019年第三季起有上漲的趨勢，它也與一般人熟知的網路釣魚電子郵件、軟體安全性漏洞，並列為三大攻擊路徑。



根據他們的調查，在黑市只需20美元，就能買到RDP帳密，以及使用RDP設備的企業網路IP位址，將這些資訊結合便宜的勒索軟體攻擊套件，就能針對開放RDP存取的個人電腦或伺服器來發動攻擊，而由於這樣的作法有利可圖、成本低，駭客很難抗拒不用。Coveware認為，除非折換現金的成功率下滑，或是促成攻擊的成本太過昂貴，否則勒索軟體與網路敲詐行為將會持續流行。

關於RDP是否為勒索軟體攻擊的主要管道，FireEye在3月16日發表勒索軟體部署趨勢時，曾剖析這類惡意程式的各種初期感染路徑，而RDP與其他遠端存取方式，就是他們最常觀測到的攻擊路徑，其次才是夾帶惡意連結或附檔的網路釣魚，以及偷渡式下載（Drive by download）。

位於英國倫敦的Beazley保險集團，也提出類似看法。他們在3月23日公布的2020年度資料外洩報告提到，當前用於部署勒索軟體的方法當中，不安全的RDP已經與網路釣魚郵件相提並論，而成為兩種最為常見的攻擊形式。

該公司負責全球BBR外洩反應服務的主管Katherine Keefe表示，企業開放員工能夠居家辦公，帶來了便利，然而，使用RDP時，若無法適當地採行正確的安全措施，將使IT系統更易受到網路攻擊的影響。

而在2019年與2020初期，BBR服務也發現，投保人系統遭洩漏的攻擊大增，正是網路攻擊IT服務代管商所致，而這些攻擊，甚至影響到一家IT服務商下游的數百個客戶，使其無法正常運作。

基於這樣的態勢，今年上半，又有幾件與RDP有關的勒索軟體攻擊被揭露。例如，微軟在3月初發表資安分析報告，他們表示，有別於Wanacry、NotPetya這類自動散播型勒索軟體，新的人為操作型勒索軟體已然崛起，他們還舉了兩個例子，分別是駭客團體

Parinacota部署勒索軟體Wadhrama的攻擊，以及多個組織使用勒索軟體Doppelpaymer發動攻擊，並且詳細解析惡意程式感染的過程，而對方發起這些行動的第一步，都是發動RDP暴力破解攻擊。

3月底，趨勢科技揭露新的勒索軟體Nefilim，散播路徑正是暴露在網際網路上的RDP設備。到了5月初，澳洲物流業者Toll Group也證實遭到Nefilim的攻擊，但3個月前他們已面臨一波勒索軟體攻擊；同一週，位於臺灣的能源產業中油、台塑，以及半導體封測業者力成科技，也傳出遭勒索軟體攻擊，法務部調查局對此提出6大檢查項目，當中就建議企業應關閉重要主機的RDP功能，似乎也暗示RDP是攻擊管道之一。

RDP安全性漏洞不勝枚舉，助長攻擊者伺機利用動機

不論是發起者是駭客、勒索軟體，RDP攻擊要能奏效，除了連網設備暴露在網際網路，以及懂得運用暴力破解帳密的手法，對方也能濫用已知的安全性弱點來進行滲透。事實上，RDP本身發展了20年，存在著漏洞這真的在所難免，從Windows NT 4.0 至今，微軟原本只在作業系統的伺服器版本，提供終端服務（Terminal Services，後來改名為Remote Desktop Services），提供RDP的使用，自Windows XP專業版起，也開始在個人電腦環境，提供RDP這類遠端存取桌面的應用，隨著Windows的重大改版，RDP也推出新版，雖然每個版本或多或少都有安全性漏洞被揭露，然而，從2019年5月14日公開的CVE-2019-0708起，局勢急轉直下。

這個被評為9.8分的重大漏洞，微軟稱為Remote Desktop Services Remote Code Execution Vulnerability，更多人以BlueKeep來代稱，是由英國國家網路安全中心（NCSC）提報的，並被資安界認為是可發展成網路蠕蟲（wormable）的漏洞，就像NotPetya與WannaCry源於EternalBlue（CVE-2017-0144）。

因為，它能讓攻擊者在不需通過身分驗證的情況下，透過RDP連上個人電腦或伺服器系統，並且傳送特製的請求──對方可在這臺設備上執行任何程式碼，隨後能來安裝應用程式、檢視、變更、刪除電腦上的資料，甚至能夠建立具有完整權限的使用者帳戶。到了5月底，McAfee、Zerodium、Kaspersky、Qihoo 360等資安廠商，也陸續針對BlueKeep漏洞濫用行為，發布概念性驗證的攻擊程式。

同年8月，又有4個同類型漏洞被揭露，也是涉及Remote Desktop Services的遠端程式碼執行（Remote Code Execution，RCE）弱點，它們分別是CVE-2019-1181、CVE-2019-1182、CVE-2019-1222、CVE-2019-1226，資安界簡稱為DejaBlue，這些也是被評為9.8分的重大漏洞。

到了11月，濫用BlueKeep漏洞的行為已經出現。例如，替BlueKeep這個漏洞命名的資安研究員Kevin Beaumont，在當時就揭露攻擊者試圖濫用BlueKeep漏洞的行為，因為，從10月底開始，在他構建的BlueKeep全球蜜罐誘捕網路環境中，所有的電腦陸續出現當機與重新啟動的異常狀況，這類事故的頻率也增加得很規律，同時，他也發現系統正在執行加密貨幣挖礦程式的檔案。微軟接獲這項通報後，也發表研究報告，證實有挖礦活動正在濫用BlueKeep漏洞。

事實上，RDP這兩年來的安全性漏洞，並非只有BlueKeep和DejaBlue，還有20個，絕大多數都是高度危險的漏洞，後續仍有可能被駭客或惡意軟體所濫用。

RDP是很危險，但其他遠端桌面軟體也有使用上的資安疑慮

從受到攻擊的熱門程度或是軟體安全性漏洞來看，無論是平時或在家辦公使用RDP，風險都相當高，然而，改用其他同類型的軟體，會比較好嗎？若就已公開的資安漏洞來考量，TeamViewer有8個，Splashtop沒有，Netop有4個，LogMeIn有4個，但VNC有121個，在2019公布的漏洞就有31個。

從產品本身提供的安全性防護機制來看，TeamViewer、Splashtop、Netop都提供256位元AES加密，以及雙因素或多因素身分認證。至於VNC系列，當中的RealVNC預設提供128位元AES加密，但可設定成256位元AES加密，以及啟用雙因素身分認證；UltraVNC則是提供資料流修改（DSM）外掛程式，讓用戶選擇使用（先前搭配MSRC4Plugin.dsm，提供128位元RC4加密，後來則改為SecureVNCPlugin.DSM，可提供256位元AES加密）。

若就過去發生的資安事故來評估，這些軟體的使用也讓人感到不安，其中，又以TeamViewer面臨的幾次爭議事件，最廣為人知，至今仍有許多人搞不清楚這套軟體是否能夠安全使用。

例如，在2016年6月，TeamViewer使用者出現帳號被侵入、冒用的狀況，對方盜用受害者電腦瀏覽器儲存的線上支付帳戶登入資訊，到亞馬遜、eBay購買禮物卡，但該公司在稍早就否認遭到侵入與資安漏洞，他們表示是使用者的疏忽所致──採用與其他帳號相同的密碼而導致TeamViewer被侵入。

到了2019年5月，德國一家新聞雜誌Der Spiegel披露，TeamViewer在2016年被駭客團體盯上而遭到攻擊，當中涉及了Winnti惡意軟體，而這樣的攻擊手法被認為與中國政府有關。

兩個月後，德國的巴伐利亞廣播公司與北德廣播公司共同發表Winnti駭客攻擊研究報告，裡面提到多家德國企業都是駭客攻擊目標，TeamViewer也名列其中，該公司也向進行這項調查的人員表示，他們徹底更換了IT基礎架構，而且在2016年為了將駭客移出他們的網路，也花費數百萬元來處理。

到了2018年4月，在免費軟體界赫赫有名的系統清理軟體CCleaner，遭遇供應鏈攻擊，而這也跟TeamViewer有關，因此讓許多人開始不信任這套工具。

根據資安業者的調查，駭客是在2017年滲透到這套產品的母公司Piriform，將惡意軟體植入新版CCleaner，隨後許多使用者下載這個版本的CCleaner，而跟著受害，結果導致230萬臺個人電腦的感染，而對方最初之所以成功滲透，就是經由TeamViewer滲透到開發人員的工作站，因為他們手上有外洩的帳號密碼，所以能夠存取該名使用者TeamViewer帳號而得逞，並在電腦上安裝惡意程式，由於這臺電腦是連接在Piriform公司的網路環境，駭客隨後可橫向移動到其他電腦進行滲透或操控。

注意遠端桌面的實體環境隱私

若不想使用RDP來連接辦公室電腦，又擔心使用其他軟體會讓其他同事看到自己操作的畫面，可考慮Splashtop，當中可針對辦公室電腦實施遮蔽螢幕與鎖定鍵盤、滑鼠的保護。

現今企業對於遠端桌面軟體的使用，除了要注意資安層面的考量，我們最後還想提醒大家注意桌面隱私的議題。武漢肺炎的疫情已持續近半年，各家公司採取的辦公方式有好幾種，除了異地辦公之外，部分公司會採取分批上班的模式，因此會出現有些人在辦公室、

有些人在家裡的狀況，若在家上班的員工是透過遠端桌面的方式連入辦公室電腦，有些軟體對於辦公室電腦螢幕，以及在家個人電腦螢幕的畫面，是以同步的方式呈現，並非以鎖定或遮蔽桌面的方式來防止他人窺伺。

根據我們的測試，像是TeamViewer、Chrome Remote Desktop，都會有這樣的狀況，Windows遠端桌面連線／RDP反而沒有，辦公室電腦一旦以此種方式被遠端連入，就會進入鎖定桌面的狀態。

Splashtop相關功能則很齊備，我們可在被控端電腦的代理程式當中設定「啟用空白螢幕」，當我們從遠端登入時，辦公室電腦螢幕就會進入全黑狀態，只會呈現滑鼠游標的位置與移動軌跡，；若擔心有人趁這時操作辦公室電腦的鍵盤和滑鼠亂搞，我們還可以勾選「鎖定鍵盤和滑鼠」的選項，所有的操作就會以遠端電腦為主。