從防毒軟體到零時差攻擊：

20 個必須了解的網路安全術語

NordVPN

「網路安全滲透到我們在網上所做的一切，網路生活比以往任何時候都更加融入我們的日常生活。因此，網路安全威脅也是對我們生活的威脅。提高自我對於網絡安全的認知，對於保護我們的利益非常重要。 每個人都可以從網絡安全術語的基礎知識學習中受益。」

Troy Hunt

NordVPN 諮詢委員會成員、微軟區域總監、開發者安全最有價值專家獎得主、troyhunt.com 部落格作者、國際網路安全演講者、Pluralsight 網站上許多高評價網站開發者安全課程的作者。

前言

如果你正準備邁向網路安全領域的第一步，那麼理解為什麼，就是起點。讓我們來看看這通常如何運作的。

你聽到間諜軟體這個名詞，你想知道這是什麼意思。從你開始尋找的那刻起，就被從未聽說過的術語所攻擊。你可能會發現這樣的定義：

> 間諜軟體是一種惡意軟體，它監視受害者的設備，在受害者不知情的情況下擷取敏感性資料。間諜軟體的例子包括：廣告軟體、鍵盤側錄器和木馬程式。

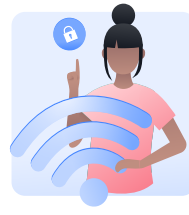
這是準確的定義，但是也沒什麼用。因為還有更多的問題出現在你的腦海--間諜軟體如何運作？什麼是敏感性資料？應該如何擔心其安全性？什麼是鍵盤側錄器？這是一個名詞嗎？

換一種方式來解釋。

相對提出技術性定義， 我們更想說明網路安全如何影響你的生活，並給到你更多實際的對比。這不是全面的詞彙表，我們希望能激發你進一步學習的欲望。

如果你想瞭解所有線上安全更詳細的技術說明，請點擊我們的部落格 NordVPN.com/zh-tw/blog，你會看到更多精彩內容。

目錄



A

Antivirus（防毒軟體）

你收到了一封新郵件。主旨是：**我愛你**

在郵件中，一個匿名仰慕者寫給你的美麗愛情告白。還附上一張照片。基於好奇心使然，你打開了附件，並下載了病毒。

你的防毒軟體會立即將其隔離。非常幸運，這是舊病毒，其特徵已在病毒資料庫中了。

如果病毒是新的且未登錄在資料庫，防毒軟體可以使用其他工具加以檢測。防毒軟體會監視電腦是否有可疑活動。如果某個程式試圖繞過防毒軟體，未經許可在啟動時執行，或下載其他惡意軟體，防毒軟體會做出反應。

而且不只是病毒。惡意軟體有很多種類：木馬程式、勒索軟體、鍵盤側錄器等：都會試圖破壞或入侵設備。

今天，「防毒軟體」一詞代表各種防止設備受到惡意軟體攻擊的反惡意軟體工具。

相關術語：病毒、惡意軟體、反惡意軟體、木馬程式、蠕蟲、廣告軟體。

B

Botnet （殭屍網路）

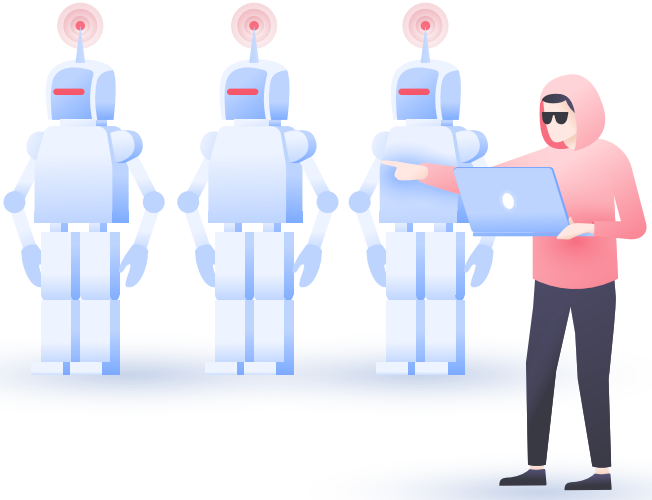
打開瀏覽器，輸入你最愛網站的網址。糟糕，網站掛了。你永遠不知道為什麼。

是僵屍造成的。

確切來說，是機器人。一大群無意識、受感染的設備向該網站發送出數十萬個請求，並使其接應不暇。

這種攻擊稱為 DDoS，全名是分散式阻斷服務攻擊。駭客使用僵屍網路來達到各種邪惡目的，例如垃圾郵件或製造虛假的網路流量。

你的設備也可能是僵屍網路的一部分，秘密執行網路罪犯的命令。很難確定你的電腦是否參與殭屍網路：唯一的跡象可能是效能稍差或過熱。



相關術語：機器人、僵屍、DDoS 攻擊。

C

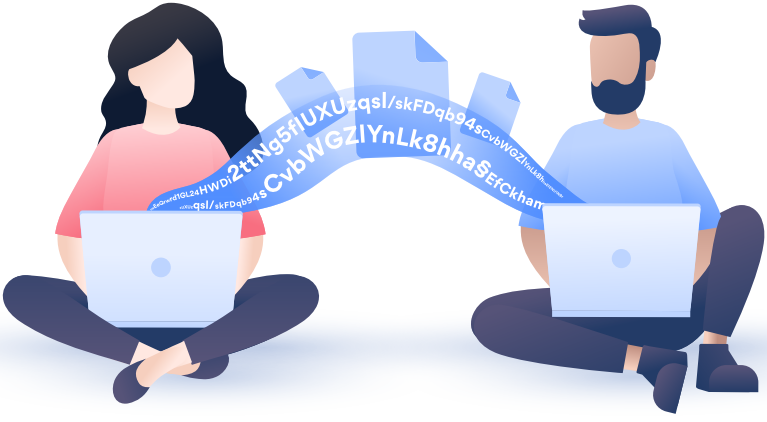
Ciphernet（密文）

你打開簡訊應用程式，發簡訊說：「抱歉，夥伴們，今晚不行。可能是胃病發作了。」

這叫做明文。它是未加密的文字，可以被線上間諜攔截和讀取。這也叫謊言：你感覺舒服，但寧願看電影。至少你正在使用一個安全的聊天應用程式。它應用一種演算法將謊言轉換成密文：

「ueEeQrwrd1GL24HWDi2ttNg5fIUXUzqsIFqb94^Ef2NU1NBrDrPb84wbReVnclTP2AgnMCkhaHC3UrfR8VWxh3jWWh+0WE」

這就是加密的作用。明文透過安全金鑰（密碼）轉換為密文。朋友使用的聊天應用程式具有解密訊息的金鑰。網路間諜沒有金鑰，無法讀取你們的通訊內容。



相關術語：加密、密碼、明文、解密。

D

Data breach（資料外洩）

你與一群最親密的朋友進行群組聊天。有一天，你注意到社群媒體上的聊天截圖。你剛剛經歷了資料外洩。

當敏感資料落入無權處理的人手中時，就會發生資料外洩。

這是怎麼發生的？駭客截獲了你的通訊？或是熟人做的？也許馬克的室友在他不在筆記型電腦旁的時候打開了聊天室。他總是看起來陰森森的。你可能永遠不會知道。

這也是發生在重大公司資料外洩事件中的情況。

公司收集了大量的資料—有時是來自像你這樣的使用者的資料—其中一些公司遭到入侵，資料被外洩，你會發現你的使用者名稱和密碼在網路上出現。

在 haveibeenpwned.com 上定期檢查你的帳戶是否因資料外洩而遭受危害。

相關術語：無意資訊外洩、資料外洩、資料洩露。

End-to-end encryption（端到端加密）

你聽到有人用歡愉的語氣說：「我們將實施端到端加密！」端到端是什麼意思？

把你的資料想像成一張紙條。在發送之前，把紙條放在信封裡，這樣可以保護內容不被竊取。這就是加密。

在途中的某個地方，第三方服務（例如，你正使用的聊天服務）打開信封，取出你的資料，並將其發送到最終目的地。

這就是網際網路的運作方式—途中都有中間人。

端到端加密去除了中間人。只有你和接收者才能看到內容。

相關術語：密文、明文。

F

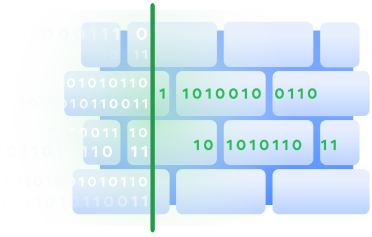
Firewall（防火牆）

你站著排隊。到達門口時，保鏢說：「不許進入。」你轉身回家：今天不能進夜店。

保鏢執行關於誰能進入和誰不能進入夜店的規則。這些規則是獨斷的：取決於夜店的政策和外部環境。例如，夜店已客滿，或者正舉辦私人派對。

同樣地，防火牆位於區域網路和網際網路之間。如同數位保鏢，它強制執行哪些流量能進入區域網路的規則。

防火牆允許來自受信任來源或 IP 位址的流量。不在名單上？抱歉，無法進入。因此防火牆可以保護網路免受可能危害系統惡意網路流量的影響。



H

Hacker（駭客）

你在電影裡見過他們。神秘、危險，甚至反社會。他們是生活在虛擬世界的數位罪犯。他們能在五分鐘內入侵五角大廈。

這顯然是虛構的。駭客是人，每個人都有自己的動機。有些人喜歡入侵網路的智力挑戰。有些人是所謂的黑帽駭客。他們懷有惡意，為了個人利益而破壞系統，竊取有價值的資料或金錢，擾亂網路，並可能造成各種損害。

許多公司和政府雇用白帽駭客，他們試圖入侵來測試電腦系統的安全性。這就是所謂的滲透測試，滲透測試可以使用多種形式：甚至是實體形式。

例如，一名白帽駭客可能跟隨一名員工進入公司大樓。他很有禮貌：通常會幫別人開門，甚至是陌生人。一旦進入，駭客可能會竊取帶有敏感資料的硬碟，存取無人監管的電腦或加以破壞（例如使用鍵盤側錄器）。

你會遭受駭客攻擊嗎？

這取決於你的安全措施。然而，技術高超的駭客往往能找到進入最安全網路的方法。好消息是，他們腦海中可能有比你 Line 帳戶更有趣的目標。

通常，你會間接遭受駭客的攻擊，請參閱：資料外洩。

你應該小心的是建立假網站並發送惡意連結的詐騙者，請參閱：網路釣魚。在詐騙網站上輸入你的密碼，就會直接把密碼交給詐騙者。

相關術語：灰帽駭客、黑帽駭客、白帽駭客、滲透、滲透測試。

Ip address（IP 位址）

你的手機具有由網路分配的 IP 位址（網際網路協定位址的縮寫）。你的筆記型電腦、智慧型電視和其他所有連網的設備也是如此。沒有 IP 位址，任何設備都無法上網運行。為什麼？

假設你需要打發時間。你拿出手機，在網址欄中輸入「Reddit.com」。

但你的手機不知道什麼是「Reddit.com」。它的母語是數字，而不是文字。要造訪 Reddit， 手機會發出一個問題：「Reddit.com 的 IP 位址是什麼？」

什麼是 Reddit.com 的 IP 地址？

該問題的解決方法是一台特殊的伺服器：一個 IP 位址資料庫。伺服器找到 Reddit 的 IP 位址，並將其發送回手機。

請求

然後，你的手機將請求發送到 Reddit 的 IP 位址。Reddit 將資訊發送回手機的 IP 位址。

Reddit 的 IP 資訊

過了一秒鐘。Reddit 就會載入到手機螢幕上。但內容無法吸引你的興趣，你按下關閉按鈕。

J

Cryptojacking（挖礦劫持）

你的電腦很熱，嗡嗡作響，風扇像瘋了一樣旋轉。而且速度很慢：必須等待一段時間才能打開任何東西。

原因是什麼？駭客劫持你的電腦來開採加密貨幣。

你可能聽說過挖礦。簡單來說，就是當你在電腦上執行複雜運算時，就會得到加密貨幣作為獎勵。但是這些運算佔用了大量的電腦能力：通常對挖礦來說，需要大量的運算能力才能獲利。

為了解決這個問題，駭客劫持設備為他們挖礦。他們透過在網頁中使用惡意軟體或惡意程式碼來執行這種稱為挖礦劫持的攻擊。使得毫無戒心的受害者不知道他們的電腦為什麼會過熱。

是的，我們知道將挖礦劫持的英文（cryptoJacking）。但是當提到網路安全術語時，這找不到 J 開頭的名詞，因此我們選擇了這個當中有 J 的名詞為代表。

相關術語：加密挖礦、 惡意加密挖掘 。

Keylogger（鍵盤側錄器）

你在圖書館為經濟學課程寫報告。昨天截止。你的筆記型電腦電池沒電了，還你忘了帶電源線。

旁邊坐著一個看起來很友善的女孩。你向她借了筆記型電腦：你需要五分鐘來完成這個想法，而這個想法還停留在你的腦海裡。她很高興能幫上忙。你拿著她的筆記型電腦，登入你的雲端硬碟，完成關於大蕭條時期反壟斷政策的報告。

回家後，你發現電子郵件和許多線上帳戶都被駭客入侵了。怎麼會這樣呢？

這個女孩的筆記型電腦上安裝了鍵盤側錄器。這是一個記錄輸入的工具。它記錄了鍵入的所有內容，包括你的雲端硬碟密碼和登入資訊。

因為你的雲端硬碟和電子郵件使用相同的密碼，駭客就可以入侵你的主要電子郵件帳戶（因此你不應該重複使用密碼）。然後駭客重置了你其他帳戶的密碼。

鍵盤側錄器很少來自看起來友善的女孩。它們通常以小型硬體裝置的形式出現，駭客將其連接到無人監管的電腦上。它們也可以是非法或合法使用的軟體工具。例如，一些公司在電腦中安裝鍵盤側錄器來監控員工。

相關術語：間諜軟體。

L

Logic bomb（邏輯炸彈）

你在工作，比截止日期晚了五分鐘。當一切都崩潰時，你正在瘋狂地打字。你無法存取內部網路或任何遠端檔案。今天無法工作了。

第二天，你聽到八卦，是一位心懷不滿的離職員工，一位 IT 人員：他關閉了內部網路。但這怎麼可能呢？他半年前被解雇，無法再存取公司的系統。

嗯，在他離職前一天，留下了一個邏輯炸彈。這是一段惡意程式碼，在滿足某些條件時啟動。例如，當 CEO 登入到敏感系統時。邏輯炸彈可以在特定的日期生效：如同我們的故事中邏輯炸彈在安裝半年後爆炸一樣。

相關術語：定時炸彈、內部威脅。

Man-in-the-middle attack （中間人攻擊）

你在一家咖啡廳，連上了公共 Wi-Fi。你剛剛向廠商發送了一封電子郵件，詢問他們的銀行帳戶。你拿到帳號，轉帳，然後喝一杯烏龍茶。

什麼？

回到咖啡廳。 一位駭客在你之前到達咖啡廳，設置了一個雙面惡魔（Evil Twin）熱點，並將其命名為「咖啡廳免費 Wi-Fi」。你相信這是合法的網路並連上它。 從那刻起，駭客就可以監控你的上網流量。

這是一個中間人攻擊行動。

駭客攔截廠商寄給你的電子郵件，並將他自己的銀行帳戶發送給你。你將錢轉到駭客的帳戶，而廠商仍在等待費用。

請注意，公共 Wi-Fi 不是安全網路。即使它不是駭客設置的，你無法知道公共網路的設定是否夠安全。有心人士可能潛伏在連線中。在連上公共 Wi-Fi 時，請務必使用 VPN。

相關術語：雙面惡魔攻擊、Wi-Fi 蜜罐。

N

Network（網路）

你的設備是網路的一部分，是更大網路的一部分，也可能是更大網路的一部分，這樣了解嗎？這就是網際網路，一個由大大小小的電腦網路所組成的網路。你的設備在其中。

離你最近的網路叫做區域網路（LAN）。這是指實體位置中的一組互連設備。所以，當你連上家庭路由器，就是連接到區域網路。

你的家庭網路很可能很小，最多可以連接十台設備（或者如果你喜歡小工具，還可以連接更多：但我們不是在評判，科技太棒了）。區域網路也可以是全公司範圍，也可以用數千個互連設備覆蓋整個學校。

相關術語：網際網路、區域網路。

P

Phishing （網路釣魚）

你收到一封來自銀行的電子郵件。 這是一個警告：有人試圖從你的帳戶中領錢。 銀行表示：「請立即發送您的使用者名稱和密碼以確認身份。」

聽起來很嚇人，但你不應該因為害怕而行動。

仔細檢查寄件人，你可能會發現不是你的銀行，而是有人假冒的。請不要回覆，不要按下電子郵件中的任何連結。直接打電話給你的銀行，詢問有關電子郵件的細節。

這種手法稱為網路釣魚。它有多種形式，主要是利用恐懼和緊迫感取得機密資訊的訊息或電子郵件。一個看起來幾乎和你的大學一模一樣的假網站。輸入你的使用者名稱和密碼，就會把登入資訊交給詐騙者。

防範很簡單：務必謹慎。小心利用你的恐懼甚至更糟的可疑資訊：承諾一些美好而不真實的事情。此外，你可以按下這裡了解更多資訊。

暫停、思考、再次檢查。如果 URL 看起來不合法，請不要按下連結。一般來說，除非你絕對確定密碼是安全的，否則不要輸入或洩露密碼。

R

Ransomware （勒索軟體）

你開啟電腦，等等，這是什麼？螢幕黑屏，但出現一條訊息：「你的檔案已經被火影忍者駭客集團加密。你有一週的時間 將500 美元的比特幣轉入我們的錢包，否則你的檔案將永遠消失。螺旋丸！」

這似乎是一部不好看喜劇的情節，但這不是開玩笑的。勒索軟體是一種惡意軟體，強制加密受害者的資料。只有駭客才能取消加密，因為他們才持有金鑰。（有很多加密協定在沒有解密金鑰的情況下幾乎無法破解。請參閱：密文、端到端加密。）

你不應該支付贖金，因為你的付款（更有可能使用加密貨幣支付，通常駭客會這樣要求）只會支持罪犯。相反地，應學習如何對抗勒索軟體：

- 不要從可疑網站下載任何東西。不要打開可疑連結、電子郵件或訊息。請參閱：網路釣魚。
- 備份最敏感的檔案。
- 更新應用程式和軟體，尤其是安全軟體。
- 使用強密碼。

S

Social engineering（社交工程）

你一大早被電話吵醒。另一端的人禮貌地解釋，他是你的網際網路服務提供者（ISP）LiteNet 的技術人員。他們發生網路故障，可能導致某些資料遺失。

是否能提供你信用卡的最後四個號碼，以便他們用於尋找你在伺服器上的記錄？

在半睡半醒之間，你就提供了信用卡號碼，並繼續補眠。兩小時後你醒來，吃了一頓豐盛的早餐，發現自己被駭客攻擊了。

打電話給你的人不是技術人員，而是精通社交工程的駭客：一個利用心理操縱來欺騙人們實施特定行動或透露敏感性資料的詐騙者。

讓我們進一步解釋。詐騙者利用早晨的時間，自我介紹以降低你的懷疑（LiteNet 是你所在地區最大的網際網路提供商，這很容易猜到），並省略了一些毫無意義的技術術語以聽起來合理。

然後他打電話給你假裝是 LiteNet 的技術人員，說他忘了他的密碼。他要你提供信用卡的最後四位數字，以確認你的身份並重置你的 LiteNet 密碼，包括 LiteNet 電子郵件帳戶的密碼。

LiteNet 是這個故事所虛構的一個網際網路提供商。但許多真正的公司可能只根據你信用卡的最後四位數字透過電話重置你的密碼。你應該在註冊時提供盡可能少的敏感資訊，並明確聲明不要透過電話發佈任何細節。

精通社交工程的駭客運用很多手法來操縱使用者，既複雜又直接。詐騙者可能會發送上千封偽造的電子郵件，希望找到一些容易上當的受害者，並希望他們回覆信用卡詳細資訊或密碼。請參閱：網路釣魚。

Two-factor authentication （雙因素驗證）

你在朋友的手機上登入 Facebook，因為你把自己的手機忘在家裡了。因為 Facebook 認為這是一個新設備，你需要在自己的手機上使用特殊的身份驗證應用程式來確認登入，但你的手機不在身邊。

哎呀，這是網路安全的困境！

沒錯，這可能會為你帶來一些不便，但雙因素驗證（2FA）提供了第二層保護。如果你在沒有手機的情況下無法存取你的帳戶，駭客也一樣無法入侵你的帳戶。

雙因素通常是：

你知道的東西（密碼或 PIN 碼）。
你擁有的東西（電話、編碼簿或你的生物特徵）。

沒有任何系統是牢不可破的，但 2FA 將帳戶的安全性提升到超出多數使用者擁有的安全性。網路駭客通常會投機取巧，因此他們不會試圖繞過 2FA，而是會選擇其他目標，他們偏好針對使用 ABCDEFG 作為密碼的人。

你應該在所有支持 2FA 的服務上啟用 2FA。這是簡單的方法，可以在最少不方便的情況下實現更安全的線上服務。

相關術語：多因素驗證。

V

VPN （虛擬專用網路）

你瀏覽、捲動、網路漫遊。每次你上網，都會留下一些關於你自己的資訊。你的網際網路服務提供者可以存取你的線上流量。你存取的每個網站都可以看到你的 IP 位址。

這不只是隱私問題，還關係到你的線上安全。許多網站仍未使用安全通訊協議。多數應用程式都沒有透露他們採用何種網路安全措施。你只能毫無理由地信任他們。

VPN（虛擬專用網路）是一種工具，可透過安全伺服器引導所有流量，在此過程中對其進行加密，並更改 IP 和虛擬位置。儘管聽起來有些技術性，但 VPN 是一種主流工具，一般人也很容易上手。

這不代表所有市面上的 VPN 都很棒。VPN 將你的所有流量路由到其伺服器，因此可以收集你的資料並將其出售給出價最高的競標者。好消息是，多數最大的虛擬專用網路都是透明的，沒有使用者紀錄，因此沒有任何東西可以出售或洩露給協力廠商。

例如，我們 NordVPN 的無日誌政策和服務由四大會計公司定期稽核。

相關術語：定時炸彈、內部威脅。

Wi-Fi

你在飯店房間裡，透過免費的 Wi-Fi 上網。樓下一位駭客正在監視你的線上活動。怎麼會這樣？

公共 Wi-Fi 本質上是不安全的：網路罪犯可以使用多種方法來利用或入侵。

如果路由器設定不當，駭客可以觀察任何公共 Wi-Fi 使用者的上網流量。或者駭客可能會找到透過網路將惡意程式碼注入裝置的方法。

駭客可能會設定一個假熱點：雙面惡魔（evil twin），並誘騙你連上這個假熱點。請參見：中間人攻擊。

你的安全程度取決於：

飯店 Wi-Fi 的設定和安全措施。
你造訪的網站和使用的應用程式的安全措施。
你的個人網路安全措施。

你通常不會知道公共網路是否安全，因此在連上公共網路時應避免存取敏感性資料。為何不改用行動數據呢？或者打開 VPN？

另外，如果你正在規劃活動，請不要依賴場所提供的 Wi-Fi，因為它很少是安全的。正確設定 Wi-Fi 熱點絕非易事，需要精確的技術知識。如果你不具備相關技術能力，最好雇用專業人員。

但你的工作同樣重要：你需要溝通！通知活動參與者有關官方熱點的資訊，並警告他們不要連上任何其他熱點，即使它們看起來是合法的。

相關術語：惡意軟體注入、Wi-Fi 偵測。

Z

Zero-day exploit （零時差攻擊）

你更新了軟體，安裝了防毒軟體，打開了防火牆。在這一刻，沒有駭客可以侵入你的系統，是這樣嗎？

要是這麼簡單就好了。

電腦網路、軟體和硬體都是由人們創造的。人們會犯錯誤，他們不會考慮所有可能的情況，他們會留下漏洞。

駭客利用這些漏洞。他們尋找系統中的弱點並入侵。

一旦發現漏洞，就要對其進行修補。你為應用程式或作業系統安裝的更新通常只是針對新發現漏洞的修補程式。

（當然，有些漏洞永遠無法修補。在網路安全方面，最弱的環節往往是人，而不是機器。請參閱：社交工程。）

供應商不知道零時差攻擊，因此未對其進行修補。該名稱指的是供應商修復漏洞的天數：零天。基於此漏洞的攻擊稱為零時差攻擊或零日攻擊。

因此，即使保持系統的安全、修補和更新，零時差攻擊也可能透過以前未知的漏洞危害系統。解決辦法是不斷提高警覺。上網時要聰明，使用強密碼，如果你不確定連結是否安全，不要按下連結。

這樣就能最大程度降低風險，迫使駭客尋找其他更容易的目標。

相關術語：零時差漏洞、零時差攻擊。