趨勢科技研究報告

鎖定目標攻擊所使用的後門程式技巧

Dove Chiu、Shih-Hao Weng 與 Joseph Chiu
鎖定目標攻擊防禦研究團隊

內容

簡介.....1

後門程式技巧.....2

連接埠綁定.....2

防止連接埠綁定的手法.....4

反向連線技巧.....4

防止反向連線的手法.....4

利用可用連線.....4

防止利用可用連線的手法.....6

利用合法平台作掩護.....7

防止利用合法平台作掩護的手法.....9

利用常見服務通訊協定/檔案標頭.....9

防止利用常見服務通訊協定/檔案標頭的手法.....10

變換通訊協定.....10

防止變換通訊協定的手法.....13

利用自訂 DNS 查詢.....13

防止利用自訂 DNS 查詢的手法.....14

趨勢科技法律免責聲明

本文之內容僅供一般資訊及教育用途。不作為也不應視為法律諮詢建議。本文之內容可能不適用於所有情況，也可能未反映出最新的情勢。在未就特定事實或所呈現之情況而徵詢法律建議之前，不應直接採信本文之所有內容或採取行動。趨勢科技保留隨時修改本文內容而不事先知會之權利。

所有翻譯成其他語言之內容僅供閱讀之方便。翻譯之準確性無法保證。若有任何關於翻譯準確性的問題，請參考本文件原始語言的官方版本。任何翻譯上的不一致與差異皆不具約束力，且在法規與執法上不具法律效力。

儘管趨勢科技已盡合理之努力確保本文內容之準確性與時效性，但趨勢科技對其準確性、時效性與完整性不提供任何擔保或聲明。在您存取、使用及採納這份文件內容時，即同意自行承擔任何風險。趨勢科技不提供任何形態之擔保，不論明示或隱含之擔保。趨勢科技或建立、製作或供應此文件之任何相關對象，對於存取、使用、無法使用、因使用本文、因本文內容之錯誤或遺漏而引起之任何後果、損失、傷害皆不承擔責任，包括直接、間接、特殊、連帶、營利損失或特殊損害賠償。使用本文之資訊即代表接受本文之「原貌」。

利用已開啟的連接埠.....14
防止利用已開啟連接埠的手法.....15
結論.....15
參考資料.....16

簡介

所謂的「後門程式」是一種能在電腦上開個後門讓駭客從遠端進入電腦的應用程式，這類程式在鎖定目標攻擊當中扮演著關鍵的角色。[1] 它們通常用於鎖定目標攻擊程序的第二階段 (突破防線) 或第三階段 (幕後操縱 [C&C])，後門程式可讓駭客取得目標網路的幕後掌控權。[2]

後門程式能讓駭客在不被發現的情況下與其目標網路建立連線。事實上，研究發現，許多鎖定目標攻擊所用的後門程式皆已經過精心設計，能躲過任何一種入侵防護系統 (IDS) 的偵測。[3]

後門程式有多種技巧可以讓駭客取得目標網路的幕後操縱能力，了解這些技巧將有助於 IT 系統管理員更有效地偵測後門程式，並防止自己所管理的網路遭到鎖定目標攻擊。

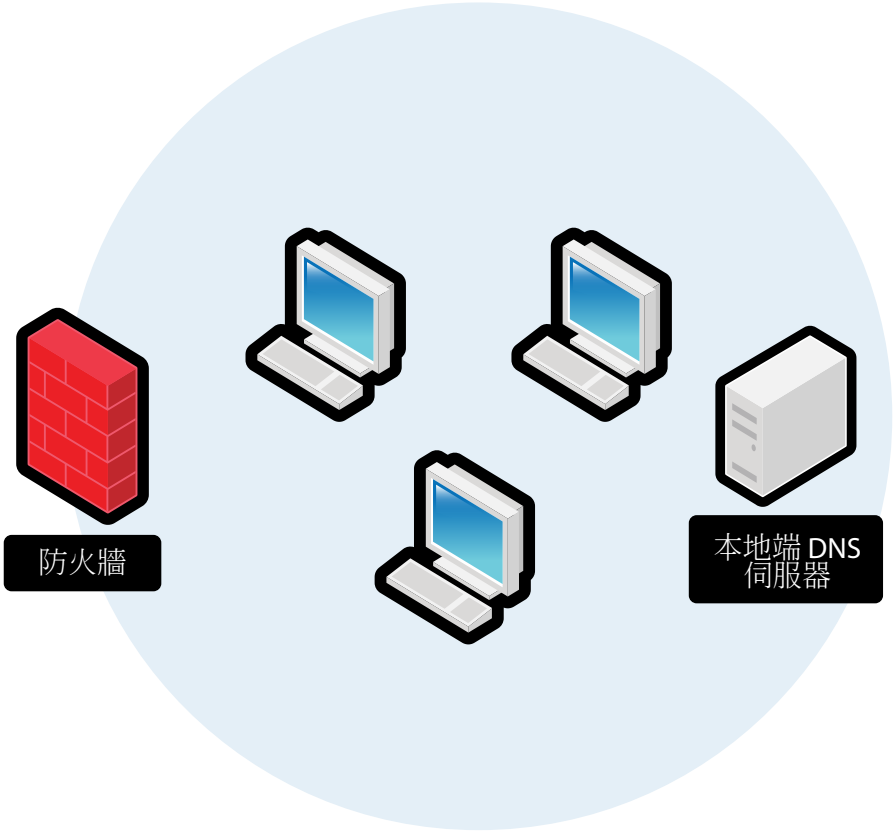

圖 1：典型的企業網路架構。

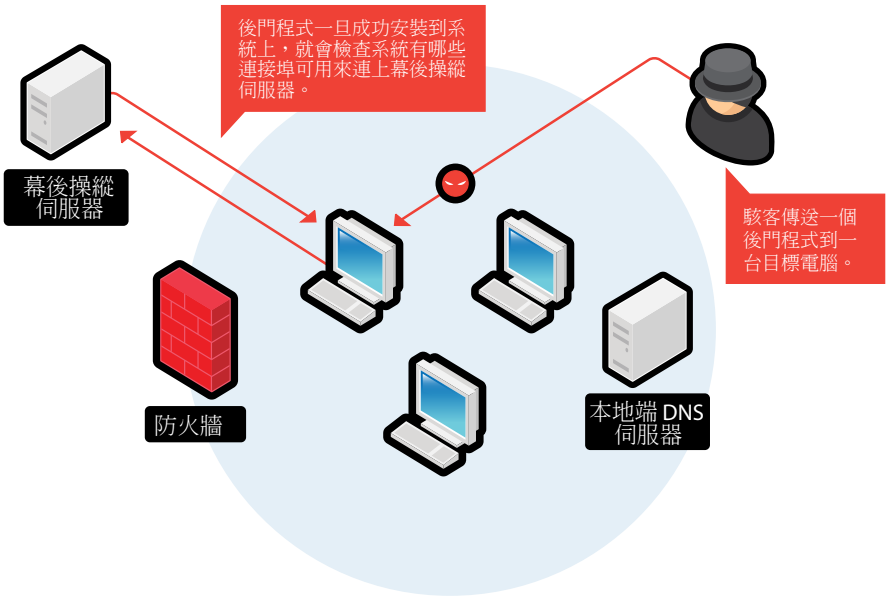

圖 2：典型針對企業網路的鎖定目標攻擊。

後門程式技巧

連接埠綁定

「連接埠綁定」一種是指定訊息收發管道的設定，在防火牆尚未普及於企業網路之前，這是一種常見的駭客手法。[4] 過去，絕大多數的伺服器皆使用公開的 IP 位址，因此很容易遭到攻擊。

駭客利用此手法來設定後門程式經由 (或綁定) 某個伺服器連接埠來直接進行通訊，這樣可以更輕易掌控該伺服器。一旦搭起連線，後門程式就會啟動一個指令列介面程式 (shell) 來執行命令。

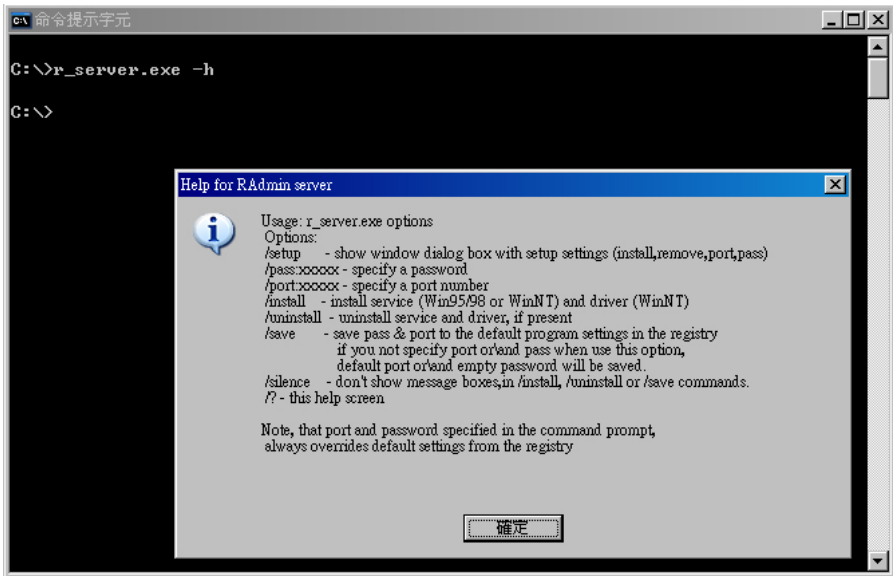

圖 3：修改過的 Radmin® Server 軟體改用指令列介面而非圖形使用者介面 (GUI)。

一個使用連接埠綁定技巧的熱門應用程式是 Radmin Server 遠端管理程式。[5] 它原本是設計給技術支援人員使用的一種遠端存取軟體，但駭客已修改了 Radmin Server 的元件來作為滲透目標網路的工具。[6] 一般的改法都是將它轉成非圖形使用介面程式。

現在，儘管防火牆已經是企業網路的一項基本配備，但還是有些企業並未採用，因此這些企業就有可能遭到連接埠綁定手法攻擊。

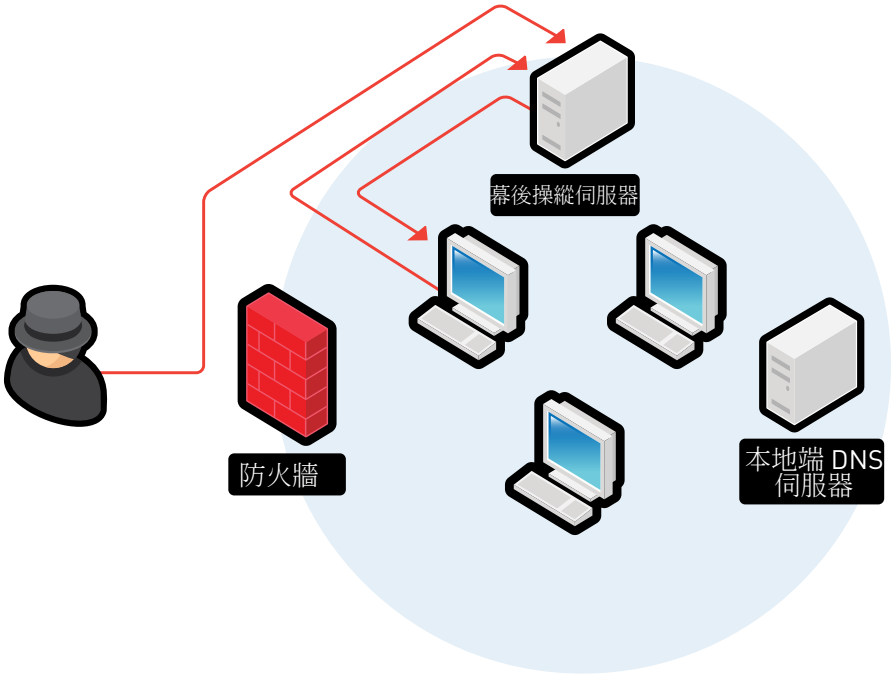

圖 4：連接埠綁定如何運作。

防止連接埠綁定的手法

IT 系統管理員可架設防火牆來阻止後門程式接受外部連線，進而防止利用連接埠綁定手法的攻擊。

反向連線技巧

駭客經常使用一種稱為「反向連線」的技巧來穿越防火牆。[7] 駭客會利用受害者電腦上的後門程式來連上歹徒的幕後操縱 (C&C) 伺服器，然後再經由企業防火牆所開放的連接埠來連回受害者的電腦，這樣就能躲在目標網路當中而不被發現。

為了通過企業防火牆，駭客必須先將一個後門程式送到目標網路，這樣才能將受害者系統連上幕後操縱伺服器，然後再連回目標系統。不過此技巧仍需躲過其他防護措施，例如惡意程式防護軟體。駭客通常會利用電子郵件來將後門程式傳送至目標。[8] 此外，駭客也經常會入侵一些使用公開 IP 位址的伺服器，用來當成幕後操縱伺服器，以免暴露其真正位置。

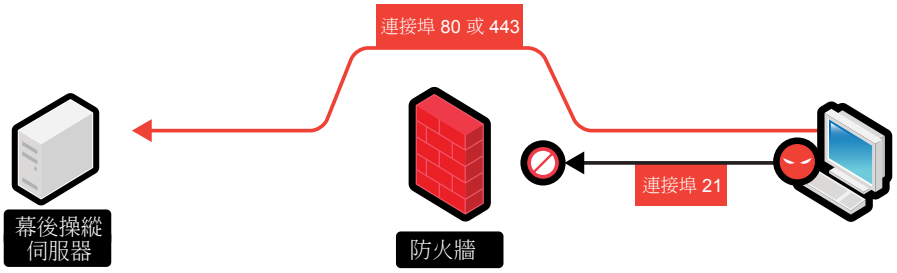

圖 5：反向連線技巧如何運作。

防止反向連線的手法

在網路及端點裝置上安裝防火牆和入侵防護 (IDS) 能讓 IT 系統管理員有效防止企業遭到反向連線技巧的攻擊。此外，必要時連續監控對外可疑連線以觀察是否加以封鎖或深入調查，也會有所幫助。

採用電子郵件掃瞄和過濾解決方案來攔截含有惡意附件或惡意 URL 的電子郵件，同樣也有所幫助。趨勢科技 InterScan™ Messaging Security、趨勢科技 Deep Discovery 以及趨勢科技 ScanMail™ Suite for Microsoft® Exchange™ 都是不錯的解決方案。[9、10、11]

利用可用連線

駭客通常會使用好幾個惡意程式作為滲透及長期潛伏在目標網路的工具，同時也用來從目標網路取得機密資料。例如，駭客可能使用某個惡意程式來滲透目標網路，然後再利用另一個惡意程式來長期潛伏在網路內竊取資訊。[12]

一開始的惡意程式，也就是「第一波後門程式」，主要負責下載其他惡意程式，也就是「第二波後門程式」，由第二波後門程式負責竊取資料。在這類攻擊當中，第一波程式會確保第二波程式成功安裝在目標系統且不被偵測。在某些情況下，駭客會使用不同的幕後操縱伺服器來操縱第一波和第二波後門程式，讓兩者維持獨立運作。

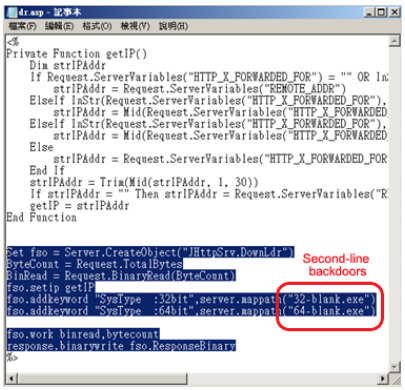

圖 6：鎖定目標攻擊用來當成第二波後門程式的伺服器程序檔 (script)。

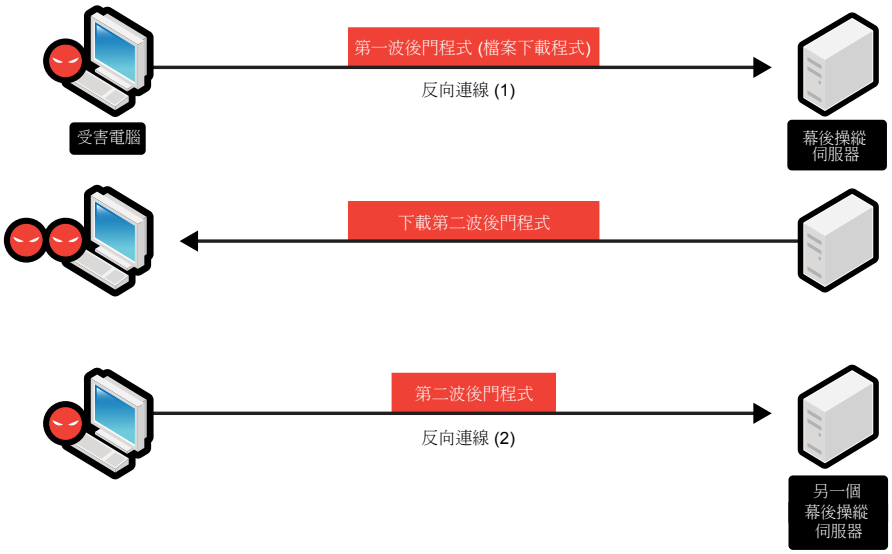

圖 7：第一波和第二波後門程式在鎖定目標攻擊當中彼此合作。

為確保最終的程式能在目標系統上執行，駭客會不時利用 Ping 或 Netcat 來檢查幕後操縱伺服器的連線是否正常，Netcat 是一個網路工具程式，可經由網路連線來讀寫資料。[13]

不過在某些情況下，就算能夠與幕後操縱伺服器連線，也不代表駭客能躲過網路上所安裝的入侵防護系統 (若有的話)。我們曾見過駭客利用一些內建 Netcat 類似功能的後門程式 (如 TSPY_DESLOC.AA)，來嘗試在不被入侵防護系統偵測到的情況下與幕後操縱伺服器建立連線。[14]

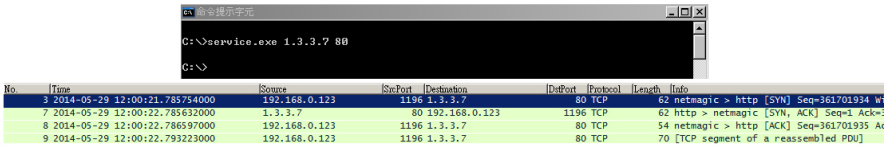

圖 8：後門程式在程式碼當中插入額外參數，試圖在不被入侵防護系統偵測到的情況下連上幕後操縱伺服器 (螢幕畫面是在後門程式於模擬網路環境中執行時所擷取)。

在一些利用這項手法的攻擊當中，駭客可以很方便地切換不同的幕後操縱伺服器來檢查目標網路的下列情況：

- 幕後操縱伺服器的 IP 或網域是否已被列入黑名單？
- 目標連接埠是否有防火牆保護？
- 幕後操縱伺服器的網路特徵是否被列入封鎖？

駭客若能成功繞過前述的防護機制，就能暫時建立一個連線到目標系統來執行一些動作，例如傳輸檔案。

此外，駭客也會利用單一執行緒後門程式來滲透網路，儘管這項技巧有些限制。這類後門程式在傳輸檔案時便無法再做其他的工作 (例如躲避偵測)，因此，傳輸的檔案越大就需要越久的時間，而時間拖得越久，被發現的機率就越高。

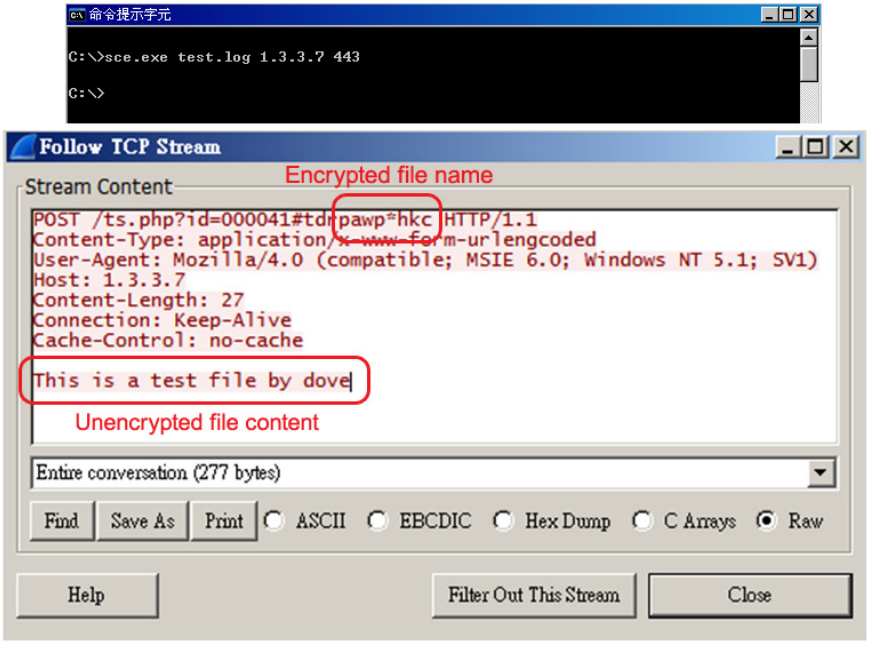

圖 9：後門程式正試圖透過連接埠 443 傳輸一個檔案到幕後操縱伺服器 (螢幕畫面是在後門程式於模擬網路環境中執行時所擷取)。

防止利用可用連線的手法

要防止這類攻擊手法，可使用一套能監控網路流量模式的資安軟體，例如趨勢科技的 Deep Discovery 就是一套有效的解決方案。不過請注意，某些後門程式的網路流量模式較難偵測，有些後門程式的網路流量更沒有明確的模式，看起來就像一般的 HTTP 通訊一樣，因此很可能造成假警報。

利用合法平台作掩護

既然後門程式的主要作用是為了讓鎖定目標攻擊能躲避資安軟體的偵測，那麼利用一些合法的平台來掩護惡意活動也就不是那麼令人訝異。其中一種方法就是利用部落格來張貼幕後操縱訊息。[15]

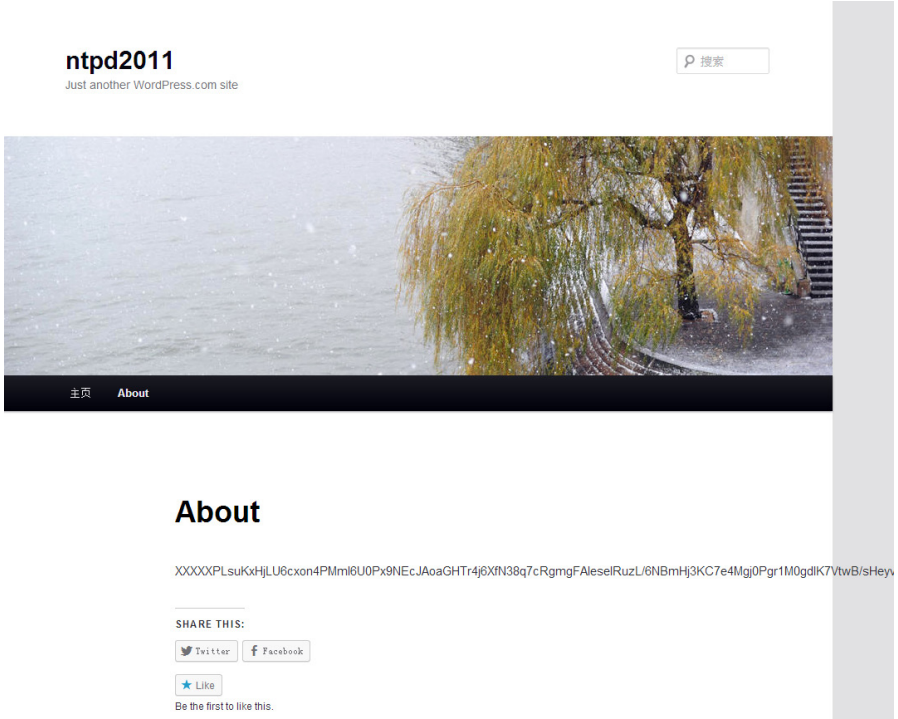

圖 10：含有加密文字的部落格頁面，文字解開之後將顯示幕後操縱伺服器的網址及連接埠。

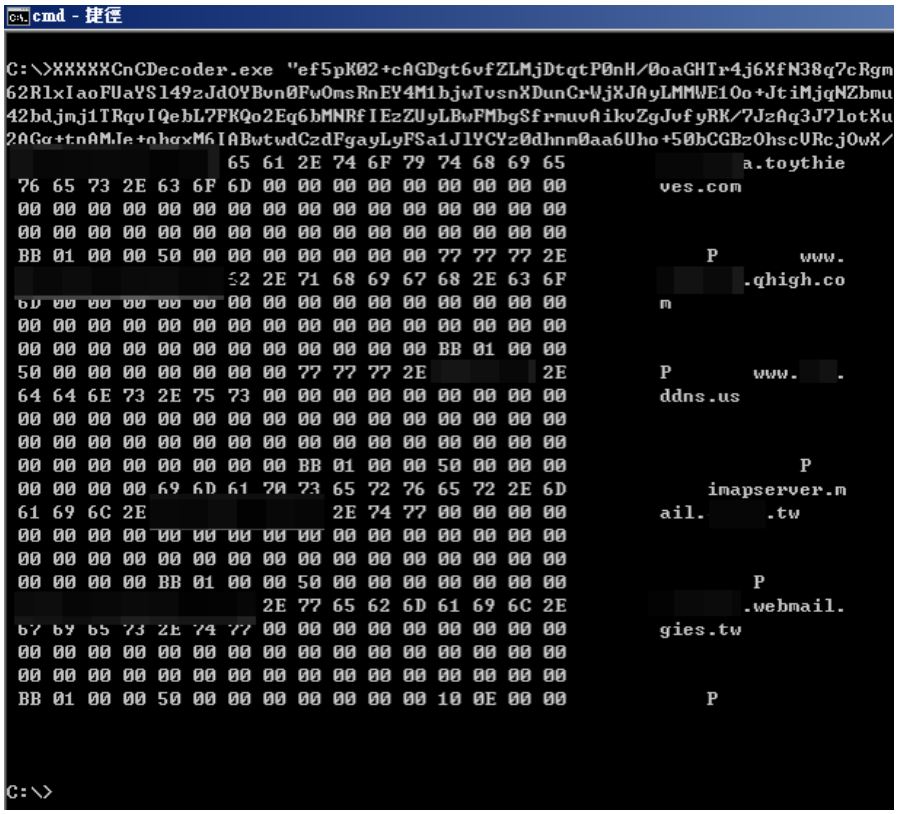

圖 11：解開後的文字顯示幕後操縱伺服器的網址清單。

在這類攻擊當中，後門程式會先連上部落格頁面來讀取加密文字，然後解開加密文字來取得幕後操縱伺服器清單。當駭客想要更改網址清單時，只需更新部落格上的加密文字即可，完全不留下行蹤。

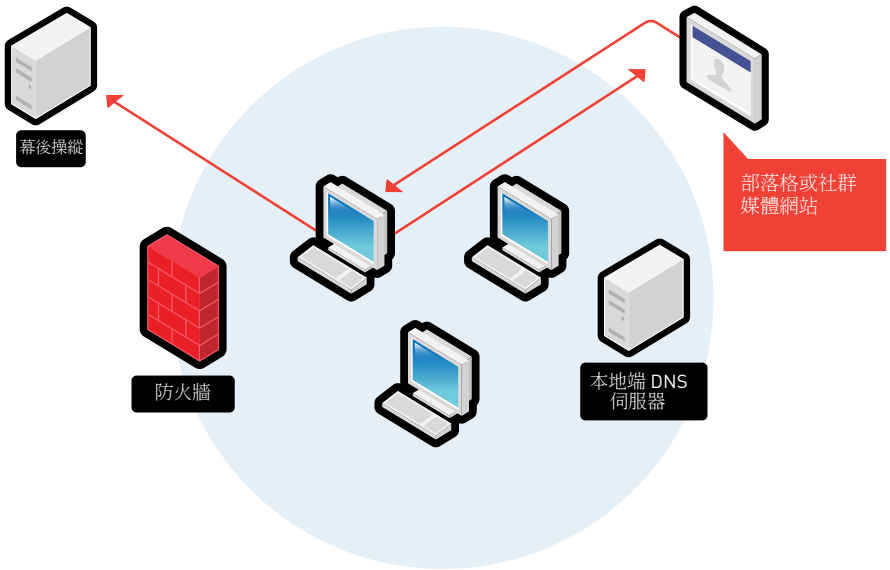

圖 12：利用合法平台作掩護的手法如何運作。

防止利用合法平台作掩護的手法

這類攻擊手法無法透過封鎖部落格或社群媒體網站的方式來防止，因為很可能造成誤判。要防止這類攻擊，必須先解開加密文字來取得需要封鎖的網域清單。此外，也可利用網路流量特徵來進行網路層次的偵測，儘管這樣的作法有可能造成假警報。

利用常見服務通訊協定/檔案標頭

駭客也會利用一般常見的通訊協定 (如即時通訊軟體和免費電子郵件服務) 來隱藏行蹤。事實上，我們已見過鎖定目標攻擊後門程式利用 Windows® Live Messenger 和 Ajax IM 即時通訊軟體協定以及 Gmail™ 郵件服務通訊協定，BKDR_DESCLOC.A 即是一例。

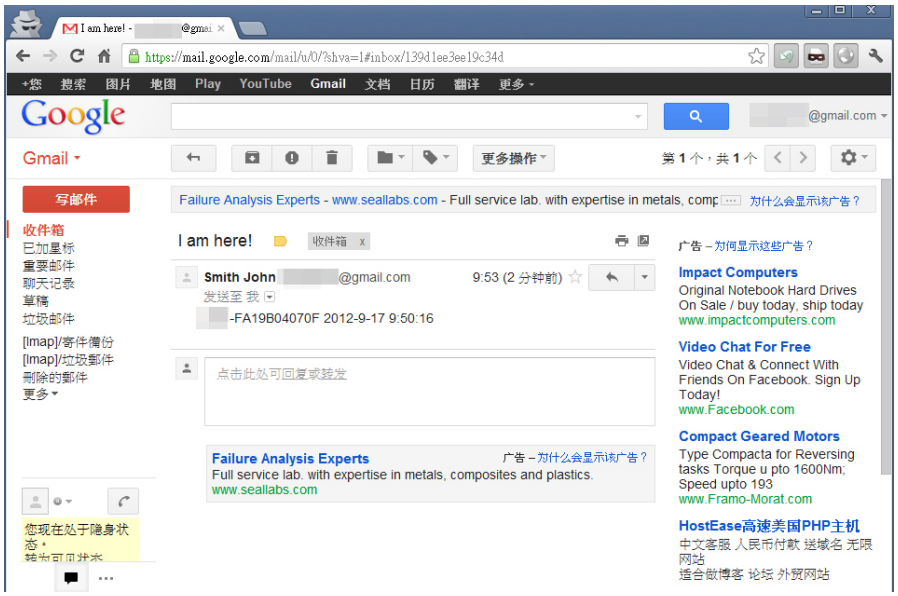

圖 13：後門程式利用 Gmail 來回報訊息。

Terminator 後門程式 (FAKEM) 就是利用這樣的手法，而且它還曾經在通訊封包的前 32 個位元組當中模仿一般常見的通訊協定和檔案標頭來試圖躲避偵測，只不過沒有成功。[16]

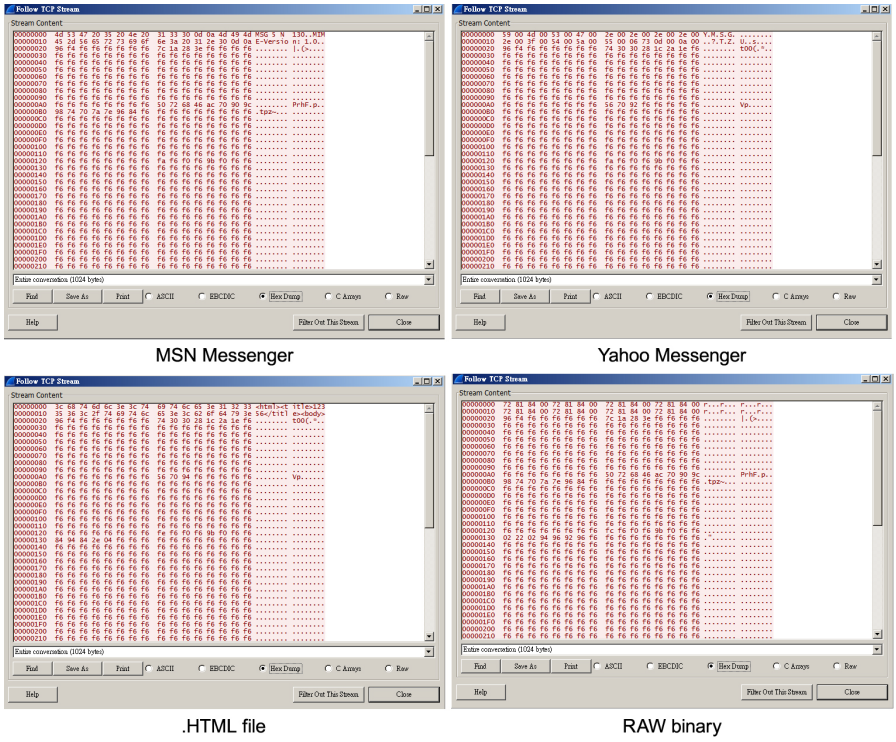

圖 14：Terminator 的幕後操縱通訊可模仿四種通訊協定的標頭。

假使後門程式模仿了整個通訊協定或檔案的標頭，那麼這類攻擊就會變得非常難以偵測。不過，駭客也必須具備非常豐富的知識。此外，這類後門程式本身也可能不太穩定，因為只要標頭稍有一點小小錯誤就可能導致它們程式不穩。

防止利用常見服務通訊協定/檔案標頭的手法

由於駭客會模仿正常的網路流量，因此，這類攻擊技巧無法從網路層來偵測。唯一的方法就是使用一套有效的惡意程式防護軟體，例如趨勢科技 OfficeScan。

變換通訊協定

除了變換幕後操縱伺服器的網址、連接埠、IP 位址或網域之外，駭客還可能變換他們所使用的通訊協定來躲避偵測。例如，PlugX 的某個變種就採用了「使用者資料包通訊協定」(User Datagram Protocol，簡稱 UDP)，而非一般常用的「傳輸控制通訊協定」(Transmission Control Protocol，簡稱 TCP)，來與幕後操縱伺服器通訊。[17] 不過，由於 UDP 通訊協定並無三向交握 (three-way handshake) 機制與阻塞管制功能，因此，後門程式在資料傳輸的開頭使用了簡化版的 TCP 標頭來防止資料遺失，確保兩端連線正常。[18]

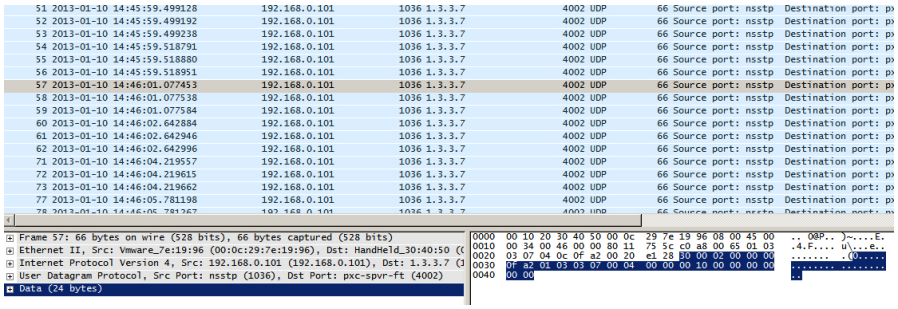

圖 15：PlugX 使用 UDP 來與幕後操縱伺服器通訊。

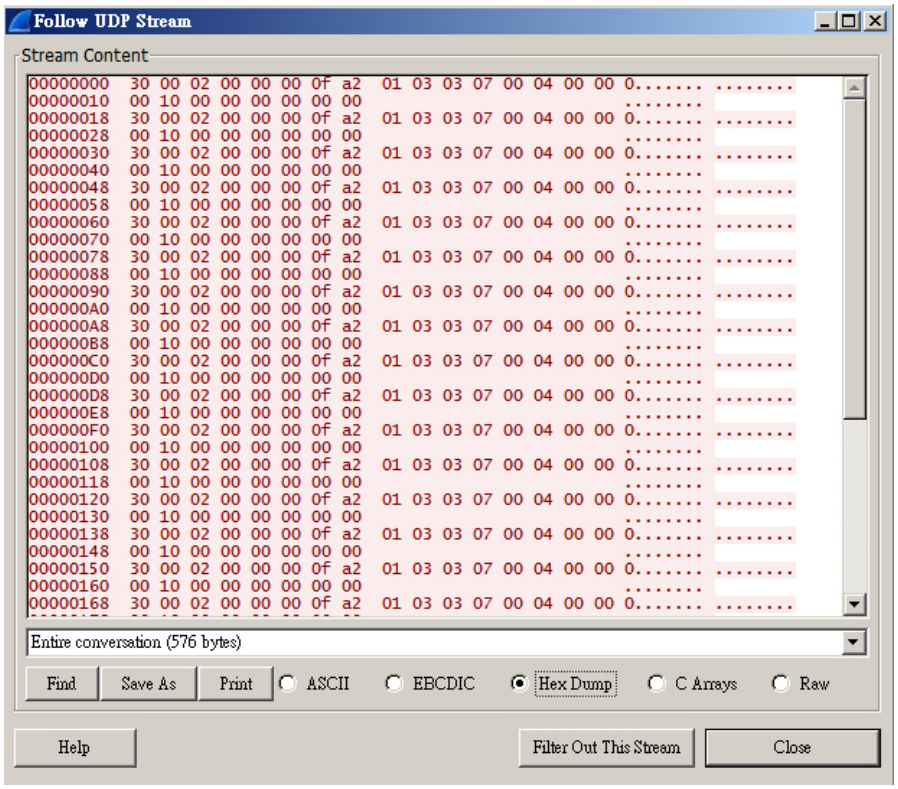

圖 16：PlugX 在 UDP 封包當中內建了自己的 TCP 標頭。

我們所發現到的樣本並未使用 UDP 來和幕後操縱伺服器溝通，而是使用「網際網路控制訊息通訊協定」(Internet Control Message Protocol，簡稱 ICMP)。 此功能已內建在 PlugX 控制程式當中，讓駭客能指定要連上哪一台幕後操縱伺服器，並可選擇使用 TCP、HTTP、UDP 或 ICMP 通訊協定。

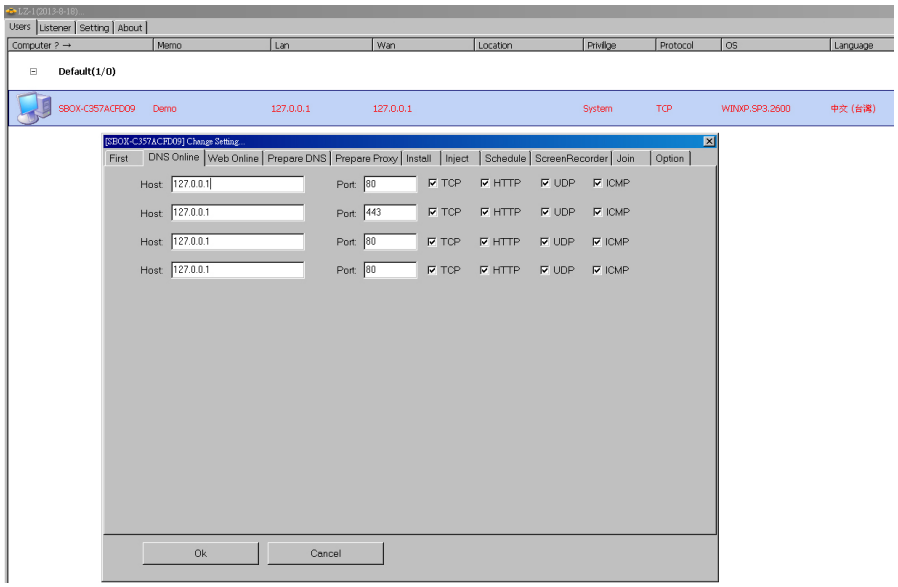

圖 17：PlugX 後門程式的反向連線設定。

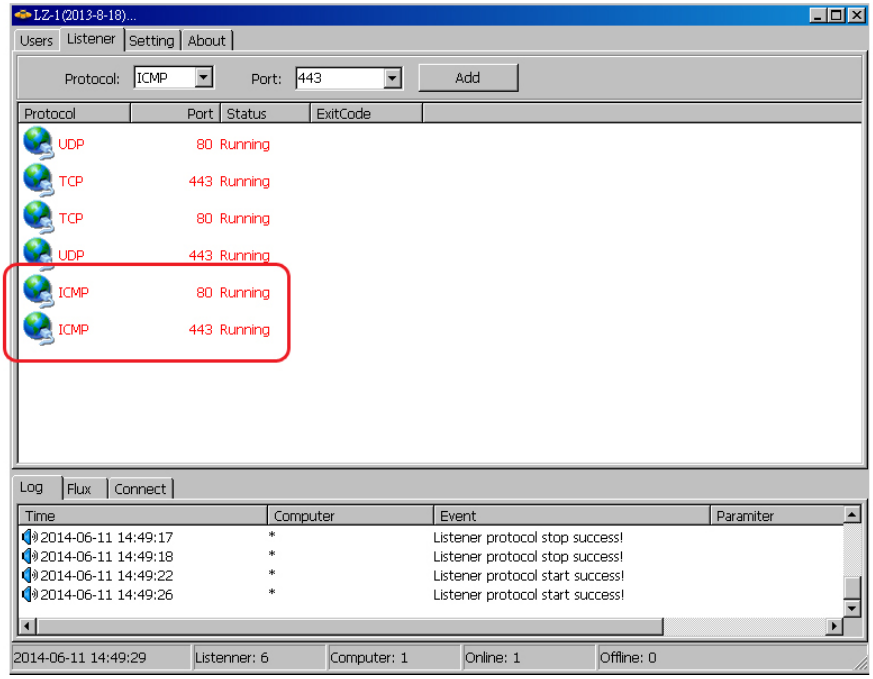

圖 18：PlugX 的控制程式可同時監聽多個連接埠和通訊協定，因此能視情況選擇適當的幕後操縱通訊協定和連接埠。

防止變換通訊協定的手法

要防止可能變換各種通訊協定來與幕後操縱伺服器通訊的後門程式，需要在防火牆上設定只開放必要的連接埠給某些通訊協定。例如，IT 系統管理員可以封鎖所有進出其網路的 ICMP 流量。雖然這是一個安全的作法，但卻有可能讓使用者非常不方便。不過，由於網域名稱系統 (DNS) 查詢通常使用連接埠 53 和 UDP 通訊協定，因此，一般來說該連接埠還是會維持開放，以防本地端 DNS 伺服器發生故障。

利用自訂 DNS 查詢

防火牆可利用黑名單機制直接針對幕後通訊伺服器的 IP 位址來加以封鎖。然而，防火牆卻無法封鎖查詢幕後操縱伺服器網域名稱的動作，因為防火牆要在 DNS 查詢之後才有辦法封鎖流量，因此一般都會改以封鎖 DNS 查詢來代替。

而駭客為了避開這樣的封鎖，他們會利用自訂的 DNS 查詢來向外部網站服務查詢幕後操縱伺服器的 IP。

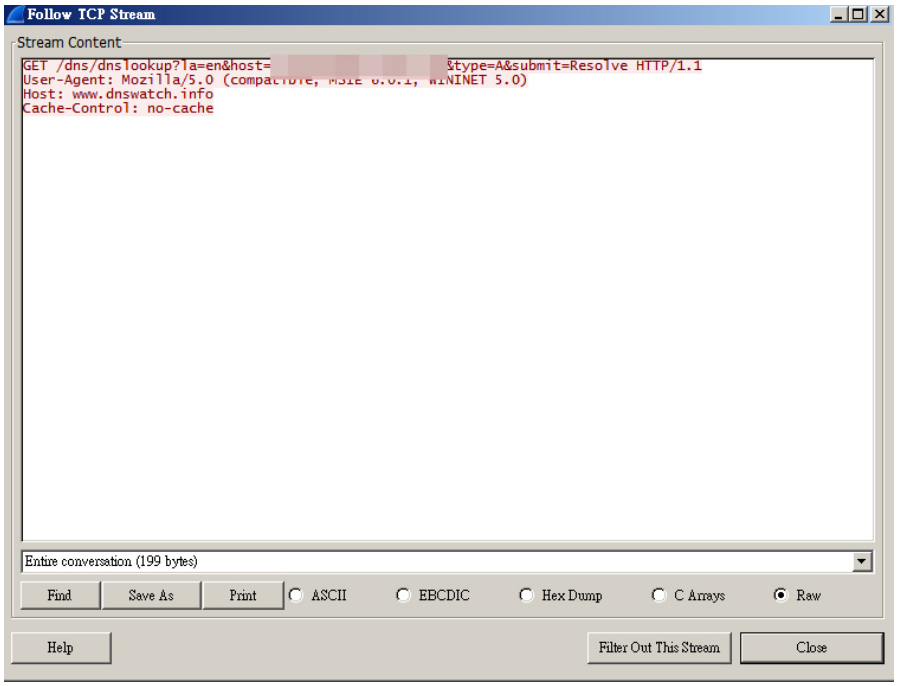

圖 19：後門程式發送到網站服務的自訂 DNS 查詢。

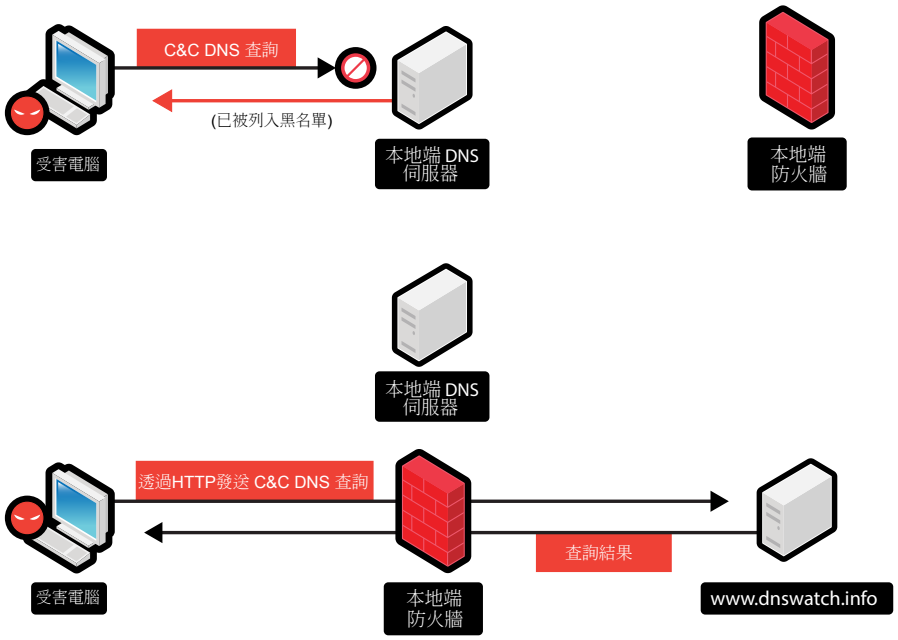

圖 20：一般 (上圖) 與自訂 (下圖) DNS 查詢如何運作。

這樣的技巧雖然簡單，但卻能讓駭客在其幕後操縱伺服器遭到本地端 DNS 封鎖的情況下，還是能夠查到其 IP 位址。此外，為了躲避偵測，他們還可以修改其伺服器的 DNS 記錄，只使用 0.0.0.0 和 127.0.0.1 兩個位址，並且趁這些位址未被使用時，才讓其伺服器開放連線。

防止利用自訂 DNS 查詢的手法

由於自訂 DNS 查詢本身並非惡意動作，因此，很難防止後門程式利用這種方法來查詢其幕後操縱伺服器的 IP 位址。IT 系統管理員必須先查出自定 DNS 查詢的伺服器 IP 位址，然後才能在防火牆和入侵防護系統上加以封鎖。

利用已開啟的連接埠

要利用已開啟的連接埠，必須透過作業系統核心模式 (也就是 Ring0) 驅動程式來執行這項動作。[19] 具備這樣能力的後門程式會利用「網路驅動程式介面規格 (Network Driver Interface Specification，簡稱 NDIS) 或 Windows 篩選平台 (Windows Filtering Platform，簡稱 WFP) 來監聽目標系統上已開啟的連接埠。利用這類後門程式，駭客就能使用任何已開啟的連接埠來通訊，而不會影響執行中的服務。

Address	Ordinal	Name	Library
000000···		FwpsInjectNetworkSendAsync0	fwpkclnt
000000···		FwpsInjectionHandleCreate0	fwpkclnt
000000···		FwpsInjectionHandleDestroy0	fwpkclnt
000000···		FwpsQueryPacketInjectionState0	fwpkclnt
000000···		FwpsInjectNetworkReceiveAsync0	fwpkclnt

圖 21：Ring0 後門程式從程式庫匯入注射封包相關的函式。[20]

透過 32 或 64 位元 Windows 系統的核心模式驅動程式，後門程式就能過濾網路流量特徵、執行指令，並且回傳結果。不過，在 Windows 7 上，駭客必須竊取到已簽署的憑證才能讓後門程式在 64 位元系統上運作。

在使用者模式 (user mode) 下也能開發出具備在 Ring3 模式下利用已開啟連接埠的後門程式。我們只要在使用者模式下使用原始通訊端 (raw socket) 來過濾後門程式的連線，就能偵測其處理程序 (process)。後門程式若註冊成一個服務提供者介面 (Service Provider Interface，簡稱 SPI) 處理程序，就會在系統登錄留下痕跡，因此就能被偵測。

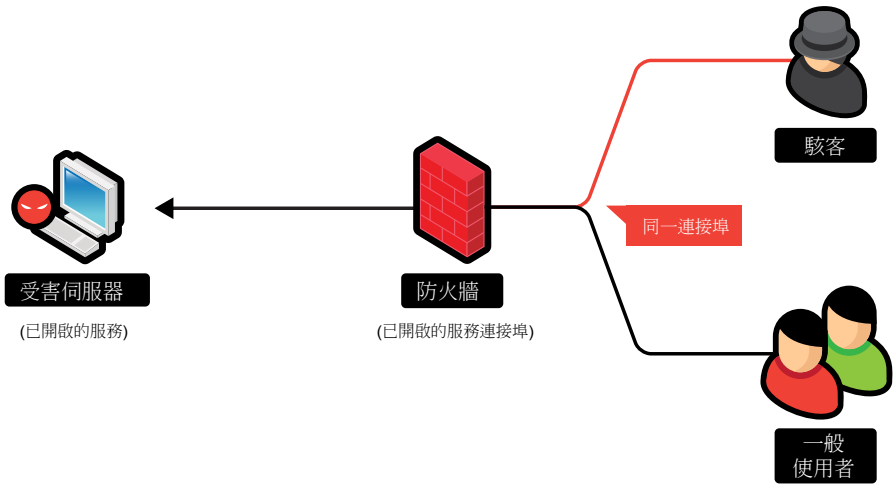

圖 22：利用已開啟連接埠的手法如何運作。

防止利用已開啟連接埠的手法

能夠利用已開啟連接埠的後門程式很難偵測，因此需仰賴具備惡意程式防護或檔案/處理程序監控功能的端點防護產品 (如趨勢科技 PC-cillin™ 和 OfficeScan™) 以及網路層的入侵防護 (IDS 和 IPS) 來提供一定程度的預防。

結論

駭客無時無刻不在精進自己的攻擊技巧，因此，企業除了防範系統和網路遭到鎖定目標攻擊之外，也必須確定 IT 系統管理員或管理團隊都能隨時掌握最新的資安發展情勢。

本文所提到的防範方法雖然無法達到滴水不漏的地步，但卻仍不失為降低駭客滲透風險的有效方法。只不過和駭客比起來，IT 系統管理員還是處於相對劣勢。IT 系統管理員必須知道網路可能遭到入侵的每一個環節，並且加以防範。反觀駭客只需在目標網路發現一項弱點就能入侵得逞。企業最弱的環節其實是「人」，因此提升安全意識是保護網路安全的一項關鍵。

簡而言之，IT 系統管理員不僅需要充分的企業網路安全知識與專業能力，還需適當的解決方案和工具，才能及時有效偵測企業網路內部潛藏的惡意活動。

參考資料

[1] 趨勢科技。(2014 年)。*威脅百科網站 (Threat Encyclopedia)*。「後門程式」(Backdoor)。上次存取時間 2014 年 7 月 10 日： http://about-threats.trendmicro.com/us/definition/backdoor。

[2] 趨勢科技。(2012 年)。*威脅百科網站 (Threat Encyclopedia)*。「偵測網路內部的敵人：APT 有多難纏？」(Detecting the Enemy Inside the Network: How Tough Is It to Deal with APTs?) 上次存取時間 2014 年 7 月 10 日：http://www.trendmicro.com/cloud-content/us/pdfs/business/white-papers/wp_apt-primer.pdf。

[3] Wikimedia Foundation Inc.。(2014 年 7 月 10 日)。*Wikipedia*。「入侵偵測系統」(Intrusion Detection System)。上次存取時間 2014 年 7 月 10 日：http://en.wikipedia.org/wiki/Intrusion_detection_system。

[4] Microsoft。(2014 年)。*Microsoft Developer Network*。「連接埠綁定」(Port Bindings)。上次存取時間 2014 年 7 月 10 日： http://msdn.microsoft.com/en-us/library/aa578247.aspx。

[5] Famatech。(2014 年)。*Radmin*。「Radmin 3 遠端遙控軟體—Radmin Server」(Radmin 3 Remote Control Software —Radmin Server)。上次存取時間 2014 年 7 月 10 日： http://www.radmin.com/radmin/rserver.php。

[6] 趨勢科技。(2014 年)。*威脅百科網站 (Threat Encyclopedia)*。「HKTL_RADMIN」。 上次存取時間 2014 年 7 月 10 日：http://about-threats.trendmicro.com/us/malware/HKTL_RADMIN。

[7] Wikimedia Foundation Inc。(2014 年 6 月 6 日)。*Wikipedia*。「Shellcode」。上次存取時間 2014 年 7 月 10 日：http://en.wikipedia.org/wiki/Shellcode。

[8] 趨勢科技。(2012 年)。*威脅百科網站 (Threat Encyclopedia)*。「鎖定目標攻擊入侵點：您的企業通訊安全嗎？」(Targeted Attack Entry Points: Are Your Business Communications Secure?) 上次存取時間 2014 年 7 月 10 日：http://www. trendmicro.com/cloud-content/us/pdfs/business/tlp_targeted_attack_entry_points.pdf。

[9] 趨勢科技。(2014 年)。*趨勢科技 InterScan Messaging Security*。上次存取時間 2014 年 7 月 10 日：http://www.trendmicro.com/us/enterprise/network-security/interscan-message-security/。

[10] 趨勢科技。(2014 年)。*趨勢科技 Deep Discovery 進階網路安全防護*。上次存取時間 2014 年 7 月 10 日：http://www.trendmicro.com/us/enterprise/security-risk-management/deep-discovery/。

[11] 趨勢科技。(2014 年)。*趨勢科技 ScanMail Suite for Microsoft Exchange*。上次存取時間 2014 年 7 月 10 日：http://www.trendmicro.com/us/enterprise/network-web-messaging-security/scanmail-microsoft-exchange/。

[12] 趨勢科技。(2014 年 5 月 12 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「鎖定目標攻擊利用最近的 Microsoft Word 零時差漏洞攻擊台灣政府機關」(Targeted Attack Against Taiwanese Agencies Used Recent Microsoft Word Zero-Day)。上次存取時間 2014 年 7 月 10 日：http://blog.trendmicro.com/trendlabs-security-intelligence/targeted-attack-against-taiwanese-agencies-used-recent-microsoft-word-zero-day/。

[13] Giovanni Giacobi。(2006 年 11 月 1 日)。*The GNU Netcat Project*。「Netcat 是什麼？」(What Is Netcat?) 上次存取時間 2014 年 7 月 11 日：http://netcat.sourceforge.net/。

[14] *VirusTotal。(2014 年 6 月 17 日)*。「TSPY_DESLOC.AA」。上次存取時間 2014 年 7 月 22 日：https://www.virustotal.com/en/file/344a75c7a364f58bb62bb6bea30024c8ae9893b31d6706d213b5a93890fdce5c/analysis/。

[15] Maersk Menrige。(2014 年 6 月 25 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「內含定時炸彈的 PlugX RAT 程式利用 Dropbox 服務來進行幕後操縱設定」(PlugX RAT with “Time Bomb” Abuses Dropbox for Command-and-Control Settings)。上次存取時間 2014 年 7 月 16 日：http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-rat-with-time-bomb-abuses-dropbox-for-command-and-control-settings/。

[16] Nart Villeneuve 與 Jessa Dela Torre。(2013 年)。*趨勢科技資訊安全情報*。「FAKEM 遠端遙控工具：惡意程式偽裝成 Windows Messenger 與 Yahoo! Messenger」(FAKEM RAT: Malware Disguised as Windows Messenger and Yahoo! Messenger)。上次存取時間 2014 年 7 月 22 日：http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fakem-rat.pdf。

[17] 。(2012 年 9 月 17 日)。*TrendLabs 資訊安全情報部落格 (Security Intelligence Blog)*。「摘除 PlugX 的功能」(Unplugging PlugX Capabilities)。上次存取時間 2014 年 7 月 22 日：http://blog.trendmicro.com/trendlabs-security-intelligence/unplugging-plugx-capabilities/。

[18] Wikimedia Foundation Inc.。(2014 年 7 月 17 日)。*Wikipedia*。「傳輸控制通訊協定」(Transmission Control Protocol)。上次存取時間 2014 年 7 月 16 日：http://en.wikipedia.org/wiki/Transmission_Control_Protocol。

[19] Wikimedia Foundation Inc。(2014 年 7 月 15 日)。*Wikipedia*。「保護圈」(Protection Ring)。上次存取時間 2014 年 7 月 17 日：http://en.wikipedia.org/wiki/Protection_ring。

[20] Microsoft。(2014 年)。*Windows Dev Center—Hardware*。「封包注射函式」(Packet Injection Functions)。上次存取時間 2014 年 7 月 17 日： http://msdn.microsoft.com/en-us/library/windows/hardware/ff569975(v=vs.85).aspx。

趨勢科技為資訊安全軟體全球領導廠商，致力創造一個安全的資訊交換世界。我們創新的解決方案能為消費者、企業及政府機構提供多層式的內容安全防護，涵蓋行動裝置、端點、閘道、伺服器以及雲端。我們所有的解決方案皆以趨勢科技 Smart Protection Network™ 的雲端全球威脅情報為後盾，更有全球 1,200 多位威脅情報專家在背後支援。如需更多資訊，請至： www.trendmicro.com。

©2014 年版權所有。趨勢科技股份有限公司保留所有權利。Trend Micro 與 t 字球形標誌是趨勢科技股份有限公司的商標或註冊商標。所有其他公司和產品名稱為各該公司的商標或註冊商標。

TREND MICRO™

Securing Your Journey to the Cloud

趨勢科技股份有限公司
10669 臺北市大安區敦化南路二段198號8樓
電話：(02) 2378-9666
傳真：(02) 2378-0993
網址：www.trendmicro.tw