竊取機密的隱形殺手 - 電子郵件仿冒與社交攻擊

Openfind 產品經理 林育竹

「信件匣內斗大的信件標題:『院內人事異動公告』,發信者又是高層主管,阿德不假思索地點開這封信件,又見信件內文與往常的公告格式如出一轍,便放心地開啟附件中的 PDF 檔案」,殊不知,這樣的日常舉動已經掉入最新的駭客仿冒郵件陷阱之中。

您是否有這樣的經驗:收到久未聯絡的朋友來信標題「我要結婚了!」;收到未申請的銀行信用卡對帳單「XX銀行信用卡對帳單(2010年10月)」;或者收到假冒的社群網站邀請信標題「來看看我在 Facexxxx 上的個人檔案吧」的信件,要求輸入帳號密碼做驗證,但是在執行之後才發現,已被駭客透過通訊錄的名單自動寄發大量郵件,並成為一台遭受駭客植入惡意程式的殭屍電腦,導致電腦無法使用時,才發現自己原來中毒了。

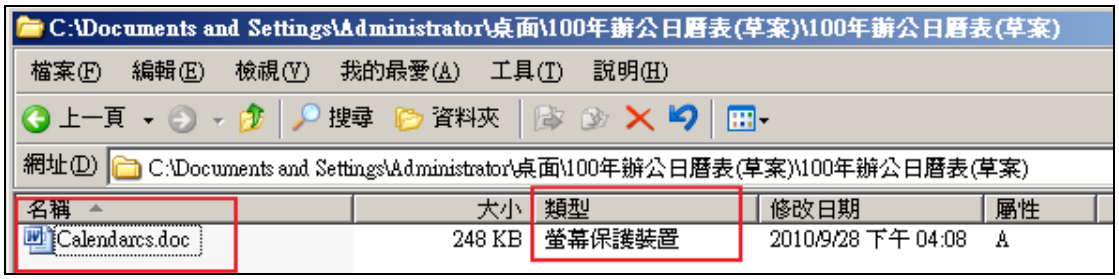
以上所舉的案例,駭客並非使用高深的資安技術,來破壞與入侵伺服器或主機,而是利用人性弱點的詐騙技術,透過具有意義的人事物,或看似正確的發信來源,來誘騙使用者上當;更甚者,會鎖定在某些特定的族群,例如政府機關或傳統產業的管理階級,這些族群對資訊安全的認知可能較為不足,但卻一樣握有組織重要資料或特殊權限,駭客最容易選擇這類族群為獵物,以竊取想要的資訊,例如帳號、密碼、相關個資隱私等,這就是所謂的「社交工程」。

日新月異的攻擊手法

社交工程的攻擊行為就像是個聰明的詐騙集團,而非暴力攻擊破門而入的強盜組織,它避開了嚴密的資訊安全硬體防護,是一種難以防範的攻擊模式,唯有集中控管或具備高度的危機意識及警覺心,才能減少社交工程攻擊傷害,是近年來令政府、企業或個人遭到重大威脅與損失的駭客慣用攻擊手法。

根據 Openfind 電子郵件威脅實驗室和 Commtouch 全球威脅爆發監控中心共同發表的 2010 第三季網路威脅調查報告顯示,這一季在台灣出現了一種嶄新的電子郵件攻擊手法,該手法是利用作業系統解讀檔案名稱時,若遇到 Unicode 控制字元,會改變檔案名稱的顯示方式進行攻擊。駭客可以在檔案名稱中,插入特定的 Unicode 控制字元,導致作業系統在顯示該檔案名稱時,誤導使用者(如圖)。

Openfind Information Technology, Inc.



攻擊者大量利用這種新式誘騙手法誘騙使用者執行惡意程式。使用者一旦誤點擊誘騙檔案，電腦隨即被植入惡意程式，駭客將可進一步控制使用者的電腦。

社交工程之所以受歡迎的原因，在於攻擊者所針對的是實際的使用者，而非機器本身的漏洞。隨著社交工程的手法日益精練，預估 2011 年垃圾郵件及郵件安全威脅也將持續成長，駭客將會以目標攻擊（Target Attacking）或魚叉式網路釣魚（Spear Phishing）為主，鎖定特定族群，引導使用者下載惡意軟體，或是誘使其在認為一切安全的情況下，無意地洩漏機敏資訊。

多重防範，給您真正的隱私安全保障

幾年來，IT 部門面臨最大的挑戰就是防治仿冒釣魚信、廣告信的課題，隨著電子郵件系統在企業中扮演越來越重要的溝通樞紐，「電子郵件安全」也隨之躍升為另一個重要議題。根據 IDC 報告顯示，84%的機密資料外洩 (不論是意外或是故意) 是由內部員工所造成，應配合組織內現行群組架構，納入主動防護的機制，由內而外落實企業郵件治理政策。

透過網路遞送資訊時最基本要注意的就是避免透過明碼方式遞送資訊，Openfind Mail2000 可以支援 HTTP、SMTP、POP3 與 IMAP4 透過 TLS/SSL 的加密傳輸協定來進行資料傳遞，由於傳遞的資料是經過加密的，就算拿到資料也無法識別內容，這樣無論透過 Web Mail 或 Outlook 之類的電子郵件工具進行信件收發，都不用擔心傳遞的資訊被有心人所擷取。

行政院資訊主任趙培因曾公開於 iThome《行政院社交工程演練擴及工友》一文中表示：「網軍攻擊只要能夠攻陷行政院內網最脆弱的環節，便形同木馬屠城、長驅直入。」（註一），因此，在今年有許多政府機關開始，對全體機關成員無預警施行社交工程演練，目的就是要減少惡意郵件開信率，全面提高使用者的資安意識。

為了更有效降低仿冒信件，Openfind 也推出公開金鑰建設（ PKI, Public Key Infrastructure）安全電子郵件解決方案，藉由專屬電子識別證的發放，使用者每次

進行登入時，必須使用個人電子識別證進行登入，發送信件時也必須加上個人簽章，以達到這封信件的身份鑑別（Authentication）、資料完整性（Integrity）、不可否認（Non-repudiation）、資料隱密性（Confidentiality），收件人可藉由解讀簽章，來驗證信件是否由信任單位所發送，或是遭到仿冒，驗證方式均遵循法規依據，能大幅降低仿冒信件的困擾。

此外，Mail2000 也支援各種安全性的機制來保護密碼不被擷取，包含密碼複雜度的設定，可以規範使用者不能設定過於簡單的密碼，並設定必須每月進行更新，登入 Webmail 時可要求輸入驗證碼，以阻擋機器人式的字典攻擊，還有提供虛擬鍵盤可以防止木馬程式側錄鍵盤輸入，或設定成一次性密碼來確保使用者身分的正確性，這些安全機制都可更加保障系統運作的安全。

如何防範社交工程的惡意攻擊？

駭客的技術已愈來愈精練，但使用者的防備心，似乎還沒有跟著全面提升，社交工程的目標對象，已從往年的組織重要人物轉移到一般職員，只要組織之中任一成員遭到滲透帳號和密碼，就可能為駭客門戶大開。

郵件傳輸的安全性可以靠加密技術來保護，但若是使用者收到的郵件中包含釣魚程式，卻是防不勝防，最安全的防護方式，仍是由系統管理者集中控管，唯有透過管理者統一設定組織內每個成員的個人環境，限制使用者可設定的功能項目，控制讀信及預覽模式、去除 JavaScript、強制純文字轉換、封鎖外部圖檔、連線失效時間等，才能有效一致地提升到組織或企業內的資安意識。

如果您擔心無法分辨電子郵件的真假，以下的檢查與設定將協助您防範大部分的社交工程惡意攻擊：

1 分析郵件主旨與附件
不開啟非公務相關的郵件以及附件。如果您收到包含附件的不明郵件，請直接聯絡發信者確認電子郵件的內容和附件後再開啟它。
2 分辨電子郵件的真偽
檢視電子郵件的信件標頭或電子簽章，查看郵件的實際發信者。
3 取消讀信預覽
避免預覽會透過 JavaScript 觸發惡意連結。
4 去除 JavaScript
完全阻絕開啟信件時自動執行內嵌的惡意 JavaScript 語法。
5 設定信件刪除後返回信件列表，避免因為自動開啟下一封信件而受到危害。

6 封鎖外部圖檔

避免因連結至外部圖檔而觸發其他連結或是受到 XSS 的危害。

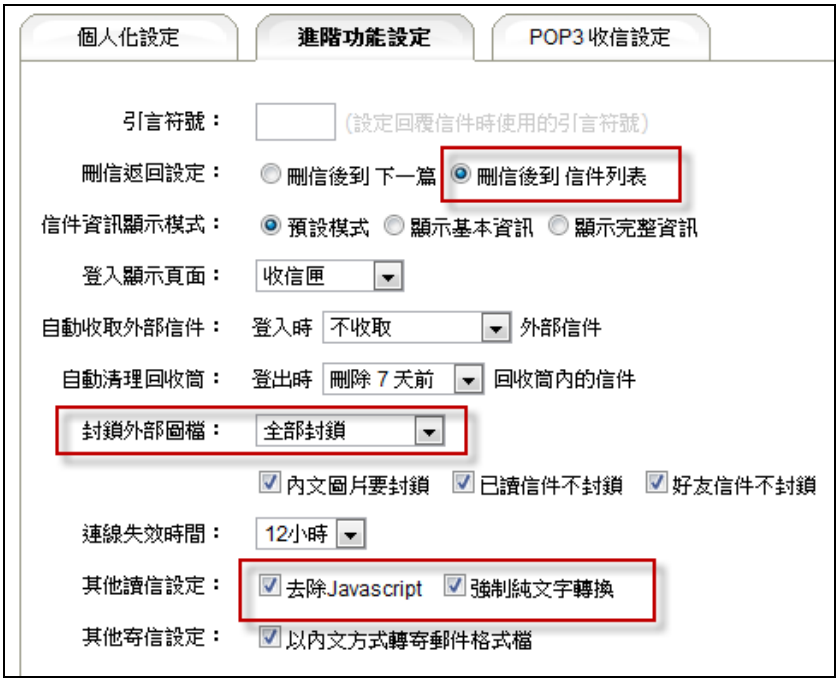
7 強制純文字讀信

將信件內容轉為純文字，讓惡意連結直接失效。

8 針對特定的信件欄位自訂過濾規則

指定寄件人、標題、信件大小等，再選擇符合條件郵件的處理方式。例如：「寄件人」,「包含」「@openfind.com.tw」，則將此信件放入「收信匣」。

9 透過權限分級控管，限制網域內成員的發信權限，以免因為不了解安全等級而不慎外流重要資訊。



為了因應持續高漲的社交工程攻擊浪潮，Openfind 也針對 Mail2000 v40 以上的版本，設計了一個安全掃描工具（SES, Social Engineering Scanner），為您組織內的電子郵件系統進行深層的資安體檢，提高系統安全建議值，這項工具即將在近期正式提供，敬請密切注意 Openfind 官方消息。

註一：行政院社交工程演練擴及工友，文/黃彥棻 (記者) 2010-08-24