SANS SECURITY AWARENESS

OUCH!

全民資訊安全意識月刊

防堵惡意軟體

概述

您或許曾聽過人們在討論網路安全時提到像是病毒、木馬、勒索軟體或是rootkit等名詞。這些都是網路犯罪者用來感染電腦和設備的各種惡意程式，又稱為惡意軟體。一旦設備被感染，網路犯罪者便能為所欲為。本期文章將介紹什麼是惡意軟體和其帶來的危險，最重要的是您能做些什麼以保護自身免受其害。

什麼是惡意軟體?

簡而言之，惡意軟體是一種用於執行惡意行為的軟體（一種電腦程式）。這是個結合了「惡意」和「軟體」的詞彙。網路犯罪份子透過惡意軟體控制您的電腦或設備。一旦被安裝了惡意軟體，駭客可以偷窺您的網路活動，竊取密碼及檔案，或是使用您的系統攻擊其他人。惡意軟體甚至能操控電腦設備裡儲存的檔案，必須支付贖金才能取回檔案。許多人認為只有Windows電腦才有惡意軟體的問題，不幸的是，不論是Mac電腦、智慧型手機、DVR或保全攝影機，惡意軟體能夠感染任何設備。受感染的電腦和設備越多，網路犯罪者便能賺越多的錢，因此包含您在內，每個人都是被攻擊的目標。

自保之道－防堵惡意軟體

有些人以為只要安裝像是防毒軟體之類的防禦程式便能安全無虞且免於被感染。不幸的是，防毒軟體無法阻擋所有惡意軟體。網路犯罪者會不斷地開發出更加複雜的新型惡意軟體以躲避檢測。另一方面，防毒軟體廠商同樣會持續更新自家產品的檢測功能。這儼然已經演變成軍備競賽，不幸的是壞人通常領先一步。既然無法只靠防毒軟體，以下提供一些可以保護自己的措施:

網路犯罪者常利用軟體中的漏洞感染電腦或設備。軟體越新，系統漏洞就越少，隨之也較不容易受到感染。請確保作業系統、應用程式、瀏覽器擴充功能以及設備保持最新版本。最簡單的方法是盡可能使用自動更新。

網路犯罪者感染電腦或行動裝置常見的方式是: 偽造電腦程式或行動裝置應用程式, 在網路上散佈後誘騙人下載安裝。因此, 建議只在受信任的線上商店下載及安裝應用程式。另外, 請避免使用全新的、幾乎沒有正面評價、很少更新或下載次數很少的Apps。還有, 該如何處理已經不再使用的電腦程式或Apps? 建議刪除!

網路犯罪者經常誘騙人們安裝惡意軟體。 例如, 他們可能會發送一封看起來正常且包含附件或連結的電子郵件給您。通常這封電子郵件看起來像是來自您的銀行或朋友, 但是, 打開附加文件或點擊連結時, 則會觸發在系統上安裝惡意軟體的惡意程式碼。因此, 如果收到的訊息帶有強烈的急迫感, 或者看起來好得令人難以置信, 那就有可能是攻擊行為。常存一份警覺之心, 以及具備相關常識往往是最好的防禦。

請定期將系統和檔案備份到網路雲端上, 或是離線儲存備份, 如分開的外接式硬碟。這樣做可以保護您的備份, 以防惡意軟體試圖加密或刪除它們。備份非常重要, 它們通常是回復受到惡意軟體感染的唯一方法。

最後, 再次提醒防範惡意軟體的最佳方法是讓所有軟體和設備都保持最新狀態, 盡可能安裝可信的防毒軟體, 並警覺任何企圖誘騙您感染自己系統的人。當以上所有措施都失敗時, 定期備份則是回復的唯一方法。

德欣寰宇為台灣專業資訊安全顧問公司。我們為客戶提供全方位安全整合解決方案。請至官方網站 http://www.tsc-tech.com/或臉書@tsctech了解更多訊息。

客座編輯

Lenny Zeltser在Minerva實驗室開發端點安全產品, 並在SANS研究院教授對抗惡意軟體相關課程。Lenny以@lennyzeltser活躍於Twitter, 並在zeltser.com上撰寫安全部落格。

參考資料

勒索軟體: https://www.sans.org/u/EdI
備份: https://www.sans.org/u/EdN
網路釣魚, 止於智者: https://www.sans.org/u/EdS

編輯委員會: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | 翻譯群: 黃意雯、宋亞倫、顧君毅、孫權劭、葉力維、莊銘輝