全民資訊安全意識月刊

OUCH!

本期話題

- 議題緣由
- 修補程式
- 備份
- 網路釣魚

WannaCry的經驗教訓

議題緣由

客座編輯
Johannes Ullrich博士 是SANS技術協會的研究院長和DShield.org的創辦人。他負責的 SANS網路風暴中心(SANS Internet Storm Center)監控現今的網路安全威脅。同時, 他教授網頁應用安全(DEV522)、入侵偵測(SEC503)和IPv6(SEC546)。

最近, 您可能已看到許多關於一個名為「WannaCry」的新型網路攻擊的新聞報導。「WannaCry」病毒感染並且鎖上了超過20萬台電腦的檔案資料, 受害範圍涵蓋各個領域, 甚至包括英國的數間醫院。這次的網路攻擊有幾個原因讓各界特別關注。首先, 它透過攻擊Windows電腦中已知的弱點迅速在電腦間散播。其次, 此種攻擊手法是使用一種稱為「勒索軟體 (Ransomware)」的惡意軟體, 這意謂著一旦您的電腦被感染, 裡面所有檔案會被加密而使得資料無法使用。恢復資料的唯一方法是以備份還原檔案, 否則須支付攻擊者300美元的贖金來解鎖。最後, 也是最重要的一點: 這次攻擊本是不應該發生的。關鍵在於Microsoft早已知悉「WannaCry」攻擊的Windows系統漏洞且在攻擊開始的數個月前便已修復並發佈了更新軟體, 但許多人並沒有及時安裝修補程式, 或者仍然使用像Windows XP這種過時且已沒有任何修補程式可使用的作業系統。為了確保不會被像「WannaCry」這樣的網路病毒感染, 以下有三個簡單步驟可供採行:

修補程式

首要步驟請確保您的電腦、行動裝置、apps和任何可連接到網路的設備皆已下載安裝最新軟體。因為網路犯罪份子一直不斷地在尋找設備中使用軟體的弱點, 一旦發現, 他們可使用特殊程式來攻擊您的設備。與此同時, 軟體設計研發公司也正致力於透過發佈更新程式來修復這些漏洞。因此, 確保電腦和行動裝置安裝更新, 將使攻擊您的難度大為提高。這也是為何WannaCry病毒的散佈如此令人沮喪。Microsoft早在兩個月前便發佈了修補和阻止此次攻擊的更新程式。如果組織能夠確保電腦更新, 這次攻擊行動永遠不會奏效。為確保您的設備

WannaCry的經驗教訓

保持最新狀態, 請盡可能啟用自動更新的功能。這個方式幾乎適用於任何會連接到網路技術的設備, 包含電腦、行動裝置、網路電視、家用路由器、遊戲機, 未來甚至有可能包括您的車子。如果您的作業系統或設備太老舊, 以至於不再支援安全更新 (如Windows XP) , 請務必汰換為可獲得支援的新設備。

保護自己免受類似WannaCry攻擊的關鍵有三個簡單的步驟: 保持電腦更新, 小心釣魚攻擊和備份您的系統

備份

在某些情況下, 像勒索軟體 (Ransomware) 這樣的網路攻擊甚至有可能會感染到最新的系統。保護自己的第二種方法是備份您的資料。備份是將電腦或行動裝置內的檔案資料另外儲存在其他地方的資料副本。這麼做的好處是當不小心遺失重要資料時, 可以透過備份復原該資料。資料備份操作容易且成本不高, 可惜大多數人並沒有定期執行的習慣。這裡將介紹備份資料的兩種存放方式: 實體裝置或雲端儲存。每種方法都有優缺點。如果您不確定何種方法合適, 可以同時使用這兩種方法。

實體裝置指的是您能夠控制的設備, 比如說家裡或辦公室使用的外接式USB或可透過網路進行存取的設備。使用實體裝置的優點是能夠快速地備份和復原大量資料; 缺點是如果不小心感染惡意軟體, 如: 勒索軟體 (Ransomware) , 有可能會擴散而影響整個備份資料。如果您使用實體裝置進行備份, 也應將備份好的副本存放在其他安全的地方, 並請確保正確地標記您儲存的任何備份。此外, 亦可選擇雲端提供的解決方案將檔案儲存於網路上。通常須先在電腦上安裝可自動執行功能的應用程式。將資料備份在雲端的優點是操作簡單。此外, 假如電腦感染到勒索軟體 (Ransomware) , 也不會影響到您在雲端的備份資料。缺點是在備份或復原大量資料時往往需要花很長的時間。另外, 也要考量雲端備份的隱私和安全性議題。試問, 您所使用的雲端服務商是否已提供足夠的安全控制措施, 例如加密您的資料和使用嚴謹的身份驗證機制?

WannaCry的經驗教訓

網路釣魚

最後, 網路攻擊手法總是不斷地日益更新。網路犯罪份子經常會使用稱為「釣魚」的方式攻擊和感染受害者的設備。網路釣魚的手法是網路罪犯向您發送電子郵件, 試圖誘使您打開受感染的附件或造訪惡意網站。如果打開了附件或進入網站, 您的電腦可能會被感染。雖然「WannaCry」沒有使用此種攻擊手法, 但它被普遍用於許多其他類型的攻擊, 包括大多數的勒索軟體 (Ransomware) 。此外, 開發WannaCry的網路罪犯無疑地會在未來幾個月內更新其攻擊方式, 並採用諸如網路釣魚等新技術來感染更多的電腦。保護自己免受此類電子郵件攻擊的關鍵是具備常識。 如果收到一封看似不尋常、可疑的或不可能是真的 (像是天上掉下禮物) 的電子郵件或訊息, 那麼很可能就是網路攻擊。

進一步了解

歡迎訂閱OUCH! 全民資訊安全意識月刊, 以及瀏覽前期OUCH!檔案。想要進一步了解SANS資訊安全意識方案, 請瀏覽我們的網站 securingthehuman.sans.org/ouch/archives.

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。

參考資料

什麼是惡意軟體:	https://securingthehuman.sans.org/ouch/2016#march2016
勒索軟體:	https://securingthehuman.sans.org/ouch/2016#august2016
備份:	https://securingthehuman.sans.org/ouch/2015#august2015
網路釣魚:	https://securingthehuman.sans.org/ouch/2015#december2015
安全的使用雲端:	https://securingthehuman.sans.org/ouch/2016#november2016

編輯委員會: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
翻譯群: 邱俊傑、黃意雯、宋亞倫、孫權劭、王澤薇、葉力維、陳月娥