電腦用戶安全意識月刊

OUCH!

本期話題

- **概述**
- **修補**
- **備份**
- **網絡釣魚**

# WannaCry的經驗教訓

## 概述

**客座編輯**
Johannes Ullrich博士是SANS技術研究所研究院院長，DShield.org創始人。他負責監控當前網絡安全威脅的**SANS互聯網風暴中心**。他在SANS教Web應用安全（**DEV522**），入侵檢測（**SEC503**）和IPv6（**SEC546**）課程。

最近，您最有可能看到一個名為“WannaCry”的新的網絡攻擊的巨大新聞報導。 “WannaCry”感染了超過20萬台電腦，將各種組織的數據鎖定，包括英國醫院在內。這種攻擊得到了很多的關注有幾個原因。首先，它通過攻擊Windows電腦中已知的弱點，從一個電腦迅速傳播到其他電腦。第二，攻擊是一種稱為“勒索軟件（Ransomware）”的惡意軟件，這意味著一旦它感染了您的電腦，它加密了所有文件，從而將您鎖定在數據之外。您可以恢復數據的唯一方法是從備份中恢復或支付攻擊者300美元的贖金來解密所有的數據。第三，最重要的是，這次襲擊本來應該是無法實現的。在Windows電腦中的弱點“WannaCry”在幾個月前一個修復程序了的知名人士已經發布 。但是許多組織無法安裝修復程序，或者仍然使用像Windows XP這樣的操作系統，這些舊版本沒有補丁不再可用。以下是您可以採取的三個簡單步驟，以確保像“WannaCry”這樣的攻擊不會感染您。

## 修補

首先，請確保您的電腦，移動設備，應用程序和其他連接到互聯網的內容都是最新的。網絡罪犯一直在尋找您的設備使用的軟件中的新漏洞。當他們發現漏洞時，他們會使用特殊的程序來攻擊您正在使用的設備。同時，為您的設備創建軟件的公司很難通過發布更新來修復這些漏洞。通過確保您的電腦和移動設備安裝這些更新，會使得別人更難以攻擊您。這就是為什麼WannaCry的傳播令人非常沮喪。能夠修復和停止此次攻擊的更新近兩個月前就已經由Microsoft發布。如果這些組織保持電腦更新，這次攻擊將永遠不會

## WannaCry的經驗教訓

奏效。為確保您的設備保持最新狀態，請盡可能啟用自動更新。這個規則適用於連接到網絡的幾乎任何技術，而不僅僅是您的電腦和移動設備，而是互聯網連接的電視，家庭路由器，遊戲機或有時甚至是您的車。如果您的操作系統或設備太舊，以至於不再支持安全更新（如Windows XP），請將其替換為支持的新的。


保護自己免受像WannaCry這樣的攻擊的關鍵是三個簡單的步驟;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，像勒索軟件這樣的網絡攻擊甚至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數據。備份是您　信息的副本存儲在您的電腦或移動設備以外的地方。當您丟失有價值的數據時，您可以從備份中恢復該數據。不幸的是，太多的人不能執行定期備份，即使它們簡單而便宜。備份數據有兩種方法：物理媒體或基於雲的存儲。每種方法都有優缺點。如果您不確定要使用哪種方法，您可以同時使用這兩種方法。

物理媒體是您控制的設備，如位於家庭或辦公室的外部USB驅動器或網絡連接的驅動器。使用您自己的物理媒體的優點是可以使您非常快速地備份和恢復大量數據。這種方法的缺點是，如果您感染惡意軟件（如勒索軟件），感染可能會傳播到您的備份。如果您使用物理介質進行備份，則應將備份的備份副本存儲在安全的位置。確保您存儲的任何備份都已正確標記。基於雲的解決方案是在線在互聯網上備份和存儲您的文件的服務。通常，您在電腦上安裝一個程序，該程序負責處理所有內容。雲解決方案的優點是它們的簡單性。此外，如果您感染勒索軟件，感染通常無法訪問您的基於雲的備份。缺點是備份或恢復非常大量的數據可能需要很長時間。您也一定要研究雲備份的隱私和安全性。備份服務是否提供強大的安全性，例如加密您的數據和強大的身份驗證?

WannaCry的經驗教訓

## 網絡釣魚

最後，壞人總是在更新和改變他們的攻擊方法。網絡罪犯經常使用另一種稱為“釣魚”的攻擊方式來攻擊和感染受害者。網絡釣魚是網絡罪犯向您發送電子郵件，試圖欺騙您打開受感染的附件或訪問惡意網站。如果您這樣做，您的電腦可能會被感染。雖然“WannaCry”沒有使用這種攻擊方法，但它通常用於許多其他類型的攻擊，包括大多數類型的勒索軟件。另外，開發WannaCry的網絡罪犯無疑會在未來幾個月內更新其攻擊方式，並採用諸如網絡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基本常識。如果一封電子郵件或訊息似乎是奇怪且可疑的或者好到難以置信，那麼很可能是一種攻擊。

## 進一步了解

歡迎訂閱OUCH!電腦用戶安全意識月刊，以及瀏覽前期OUCH!檔案。想要進一步了解SANS安全意識的方案，請瀏覽我們的網站securingthehuman.sans.org/ouch/archives.

## 參考資料

| | |
|---|---|
| 什麼是惡意軟件（Malware）： | https://securingthehuman.sans.org/ouch/2016#march2016 |
| 勒索軟件（Ransomware）： | 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 |
| 安全使用雲: | https://securingthehuman.sans.org/ouch/2016#november2016 |



編輯委員會：Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
翻譯：巴珊珊



 