電腦用戶安全意識月刊

OUCH!

本期話題

- **主要概況**
- **防毒軟件如何工作**
- **防毒技巧**

什麼是防毒軟件？

主要概況

編輯嘉賓

Jake Williams是Rendition Infosec的創始人（www.renditioninfosec.com），以及SANS的認證講師和課程的作者。他以@MalwareJake活躍在Twitter上,和撰寫他的博客malwarejake.blogspot.com。

防毒軟件是安裝在您的電腦或移動設備上, 以保護你不受惡意軟件感染的安全程序。術語 “惡意軟件” 是一個包羅萬象的代表任何類型的惡意軟件的短語, 如病毒, 蠕蟲, 木馬和間諜軟件。實際上, 術語惡意軟件來源於結合詞語惡意軟件。如果您的電腦已經感染了惡意軟件, 一個網絡的攻擊者可以捕獲所有的鍵擊, 盜取您的文檔, 或使用您的電腦攻擊他人。不同於一些人認為, 任何操作系統, 包括Mac OS X和Linux都可以被感染。您可以購買防毒軟件作為一個獨立的解決方案, 或者它通常包括作為安全計劃的一部分。問題是, 防毒不能夠跟上網絡攻擊者, 每一天他們都在不斷開發和推出新類型的惡意軟件,發布了很多的新版本。沒有防病毒程序可以檢測並防禦所有的惡意軟件。這就是為什麼您要明白非常重要的一點, 防毒軟件將幫助保護您的電腦, 它無法檢測或阻止所有類型的惡意軟件。為了更好的了解為什麼, 讓我們來看看大多數防毒軟件如何工作。

防毒軟件如何工作

一般來說防病毒軟件有兩種方法識別惡意軟件;特徵檢測和行為檢測。特徵碼檢測的工作原理是人體免疫系統。它會掃描您的電腦性能或已知惡意程序的特徵。它通過參考已知的惡意軟件詞典, 如果在您的電腦上找到與字典的模式匹配的程序就試圖壓制它來實現的。就像人的免疫系統, 詞典的方法需要更新, 比如流感疫苗, 以防止惡意軟件的新品種。防毒軟件只能防止它識別為有害的。問題是, 網絡攻擊者正在開發的新惡意軟件如此之快, 防毒軟件廠商跟不上。其結果是, 無論您最近怎麼更新防毒軟件, 總有一些可能繞過您的防病毒軟件的新惡意軟件的變種。

什麼是防毒軟件?

與行為檢測, 防毒軟件不會試圖識別已知的惡意軟件, 但是會監控電腦上安裝的軟件的行為。當一個程序可疑行為, 比如試圖訪問受保護的文件, 或者修改其他程序, 基於行為的防毒軟件軟件察覺可疑活動, 並提醒用戶。這種方法提供保護, 防止還沒有在任何字典中存在的全新類型的惡意軟件。這種方法的問題在於, 它可以產生假警報。您做為電腦用戶, 可能無法確定允許或不允許什麼, 而隨著時間的推移變得對所有這些警告脫敏。您可能會嘗試點擊 “接受” 每一個警告, 是您的電腦受到攻擊和感染。此外, 通過檢測行為的時候, 惡意軟件很可能已經在機器上運行, 在防病毒軟件識別它之前, 您可能不知道惡意軟件採取了什麼樣的行動。

雖然防毒軟件是安全的重要組成部分，它不能檢測或阻止所有的攻擊。最終，您才是最好的防守，而不僅僅是技術。

防毒軟件是以確保您的電腦和移動設備安全的一個重要組成部分, 只要有可能, 我們建議您安裝並積極地使用它。但是, 關鍵的一點要記住的是, 無論您的防病毒軟件是如何工作的, 它永遠不能保護您免受所有類型的惡意軟件。最終, 您, 不只是技術, 是對當今網絡攻擊的最佳防禦。

防毒技巧

1. 只能從已知的, 值得信賴的來源和供應商獲得的防毒軟件軟件。網絡攻擊的常見伎倆是分發假冒防病毒程序, 實際上是惡意軟件。
2. 請確保您有您的防病毒軟件, 安裝了最新版本, 您的年度訂購已支付, 並且您的防病毒設置為自動更新。如果您的電腦已脫機或關閉了一段時間, 當您重新打開它, 或者重新連接到Internet之前您的防病毒軟件需要更新自己。不要推遲這些更新。
3. 確保您的防病毒自動掃描便攜式媒體, 如USB記憶棒, 並確保即時保護處於打開狀態。

什麼是防毒軟件?

4. 注意屏幕上通過您的防病毒軟件發出的警報。大多數警報包括獲得更多信息或有關下一步該怎麼做的建議的選項。如果是您工作電腦上的警報，一定要和幫助台或您的上司立即聯繫。
5. 不要禁用或卸載防毒軟件，因為您覺得它放慢您的電腦，阻止網站或阻止您安裝一個應用程序或程序。禁用防毒軟件會帶給您不必要的風險，並可能導致嚴重的安全事故。如果問題仍然存在工作電腦上，請聯繫您的幫助台。如果問題仍然存在您的個人電腦上，嘗試聯繫了防毒軟件廠商，訪問他們的網站了解更多信息，或替換成其他防毒軟件產品。
6. 不要在同一時間在電腦上安裝多個防病毒程序。這樣做很可能會導致程序相互衝突，反而可能會降低電腦的安全性。
7. 學會識別您的防病毒軟件生成的警告。網絡攻擊者可以建立非常逼真的假的防毒軟件警告，並主動幫助您“修理”您的電腦。實際上， 點擊這些網站上的鏈接或按鈕可能會損害您的電腦。

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http://www.securingthehuman.org.

參考資料

防毒軟件產品比較:	http://www.av-test.org/en/
社會工程:	http://www.securingthehuman.org/ouch/2014#november2014
電子郵件釣魚攻擊:	http://www.securingthehuman.org/ouch/2013#february2013
我是黑客攻擊， 現在該怎麼辦？:	http://www.securingthehuman.org/ouch/2014#may2014

編輯委員會：Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
翻譯：巴珊珊