電腦用戶安全意識月刊

OUCH!

本期話題

- 什麼是惡意軟件
- 誰和為甚麼
- 保護自己

什麼是惡意軟件

主要概況

每當人們談論網絡安全時，你可能會聽到像病毒，蠕蟲，木馬或rootkit之類的術語。這些術語形容了網絡罪犯用來感染和控制電腦以及移動設備時所用的程序類型。今天，這些術語可以概括稱為惡意軟件。在這一期月刊中，我們會講解甚麼是惡意軟件，誰研製它們，為甚麼研製，還有你如何針對它來保護自己。

編輯嘉賓

Lenny Zeltser 在NCR Corp 主要集中於保護客戶的IT操作，同時他在SANS Institute教授如何與惡意軟件作戰。Lenny用@lennyzeltser的名字活躍于Twitter上，他也在 blog.zeltser.com上撰寫安全部落格。

什麼是惡意軟件

簡單的說，惡意軟件屬於軟件，又是一種用來行使惡意行為的電腦程序。事實上惡意軟件一詞就是這麼來的。網絡罪犯的最終目的是在你的電腦或移動裝置上安裝惡意軟件。一旦安裝，攻擊者有完全控制它們的可能。很多人誤解惡意軟件只是Windows 電腦的問題。Windows被廣泛使用，所以目標大，其實惡意軟件可以感染任何電腦設備，包括智能電話和平板電腦。事實上惡意軟件感染移動裝置的趨勢日益增多。而且要記住每個人都是目標，包括你。網絡罪犯感染越多的電腦和移動設備，他們就可以賺越多錢。這些網絡罪犯通常都不在乎感染了誰，只要盡可能感染更多人。

誰和為甚麼

惡意軟件不再是好奇的愛好者或業餘駭客的創造，而是尖端的網絡罪犯用來幫助他們達成某個目的。這些目的包括盜取保密數據，獲取登入和密碼，發送垃圾郵件，發起拒絕服務攻擊，勒索，或身份盜用。比如說，網絡罪犯使用像Cryptolocker這樣的惡意軟件來感染和加密你電腦裡的所有檔案。一經感染和加密，這些網絡罪犯就可以要求贖金來還取你的文件解密。

什麼是惡意軟件

創造和部署惡意軟件從而受益的，範圍可以從個人到有組織的犯罪團伙，甚至政府部門。而且，現今創造尖端的惡意軟件的人們都是以這個為目的，研發惡意軟件成為了他們的全職工作。事實上，當研發成他們的惡意軟件，他們通常會賣給其它個人或組織，同時提供定期更新和”客戶”服務。一經購買後，其它罪犯就會把惡意軟件安裝到上百萬個毫無疑心的受害者的系統上，製造成為一個由受感染系統組成的殭屍網絡。這個殭屍網絡成為一個遙控軍隊，使網絡罪犯可以用來達到自己的目的，再或者把這些受感染的電腦賣給其它網絡罪犯。

最好的辦法來抵抗惡意軟件是確保你的設備更新，盡可能用最新的防毒軟件，還有最終要對攻擊有所警惕。

保護自己

最普遍的辦法用來保護你的電腦和移動裝置不受到惡意軟件的侵害，是安裝可信的防毒軟件。防毒軟件，有時候又稱防惡意軟件，是專門用來檢測和阻止惡意軟件的。但是防毒軟件不能阻止和清除所有惡意軟件。網絡攻擊者在不斷的創新和研發能夠繞開防毒軟件的，更新更多和更尖端的進攻。與此同時，防毒軟件供應商也不斷更新他們的產品，使它有能力檢測到新的惡意軟件。從很多方面來看，這就像一場軍備競賽，雙方都想能智勝對方。可惜網絡罪犯總是占上風，因為你要知道雖然防毒軟件能夠檢測和阻止很多惡意軟件，攻擊者也總是在不斷的創造能夠被防毒軟件所忽略的新版本。所以，你不能只依賴防毒軟件來保護你，你要採取額外的步驟來保護自己。

首先，確定你的操作系統和軟件啟用了自動安裝安全更新。你的軟件越新就越難被網絡罪犯感染你的電腦和移動裝置。

其次，你是抵抗惡意軟件最好的防禦。惡意軟件的感染經常涉及社會工程學，這不外乎就是攻擊者欺騙或愚弄你來幫他們安裝惡意軟件。最常見的例子是釣魚式攻擊，這是用看似真其實是假的電子郵件來誤導你，使你感染你的電腦。比如，一個網絡罪犯寫一封電子郵件給你說是來自於你的銀行，需要

什麼是惡意軟件

你點擊信中的網址。如果你點擊了那個網址，就會被鏈接到一個能自動攻入并感染你的電腦的網頁。或者，他們寄給你一個通知，說你的包裹無法送到，要求你打開隨信的附件。當附件一打開，就會感染你的電腦。

社會工程學攻擊還會發生在其它科技產品上，比如你的電話。舉個例子，攻擊者可以打電話給你，假裝是微軟的技術服務部門通知你說你的電腦被感染了。他們的故事是騙人的，你的電腦多數也都沒有問題。他們的目的是要愚弄你使你相信你的電腦已被感染，然後再說服你給他們遙控操作你的系統的權利，或者購買他們所謂的安全軟件，實際上是個惡意軟件。你要用常識去判斷，如果一個電話或郵件顯得奇怪，可疑，或者難以相信，多數都是不可信的。

最終，最好的辦法來抵抗惡意軟件是保持你的軟件更新，安裝知名供應商所出品的防毒軟件，還有警惕某些人企圖欺騙或愚弄你來感染你的電腦。

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

OUCH 釣魚式攻擊:
www.securingthehuman.org/resources/newsletters/ouch/2013#february2013
OUCH 保護你的電腦:
www.securingthehuman.org/resources/newsletters/ouch/2012#december2012
你是目標 海報:
http://www.securingthehuman.org/resources/posters

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