電腦用戶安全意識月刊

OUCH!

本期話題

- 主要概況
- 入侵的跡象
- 如何應對

我被入侵了, 現在怎麼辦?

主要概況

我們知道你對於保護你的電腦和信息很關心, 而且採取步驟來確保它們的安全。可是, 就像開車一樣, 無論你有多小心, 難免都會遇到意外。這一期月刊裡, 我們會教你如何斷定你的電腦是否被入侵, 已及一旦發生如何應對。最終, 你越快發現電腦被入侵, 越早做出應對, 你越能減輕入侵對你或你的機構帶來的危害。

編輯嘉賓

Jake Williams (@MalwareJake; malwarejake.blogspot.com) 是CSRgroup 電腦安全顧問公司的首席科學家。他還是SANS課程「內存記憶取證(FOR526) 」和「惡意軟件逆向工程(FOR610) 」的合著者。

入侵的跡象

首先, 你要明白很多時候不是一個簡單的步驟就能斷定你的電腦是否被入侵。反而經常是通過很多跡象來確認。如果你識別出這些跡象的組合, 那就暗示你的電腦已被入侵。以下是一些例子。

- 你的防毒軟件發出電腦感染的警告, 尤其是說無法消除或隔離受感染的文件。
- 你的瀏覽器的首頁意外的改變了, 或是你的瀏覽器鏈接到一些你不願意去的網頁。
- 新的戶口出現在你的電腦裡, 而且不是你建立的。
- 新的軟件在運行, 但不是你安裝的。
- 你的電腦不斷的死機或者運行的非常緩慢。
- 你電腦裡的某個程式要求你的許可來對系統做一些改變, 雖然你沒有在安裝或更新你的應用軟件。
- 你的防火牆警告你有一個你不認識的程式正在要求鏈接互聯網的許可。

我被入侵了, 現在怎麼辦?

如何應對

如果你認為你的電腦被入侵, 越早應對越好。如果你所用的電腦是你所在機構所配置的, 不要試圖自己修理, 而且不要關機。因為那樣不單會造成傷害多過幫助, 而且可能會毀滅有價值的證據用以做調查研究。反而, 你應該立刻向你的上級匯報, 通常是聯絡你的客服部門, 安全部門, 或上級。如果你無法聯絡到你的機構, 或者你擔心延誤, 你可以斷開網絡鏈接, 然後把你的電腦設定到睡眠, 暫停或休眠模式。就算你不確認是否被入侵, 你最好還是儘早匯報以防萬一。你的機構多數已經有一套措施和隊伍專門來處理此類問題, 所以交給他們來處理。

你的電腦遲早都會被入侵, 你越快發現就能越快應對, 就越好。

如果被入侵的電腦是你私人的, 你可以嘗試以下這些步驟。

- **備份**。你能做的最重要的步驟環節是提前備份。特別要經常備份你的資料數據, 而且隨時檢查你能夠從備份裡恢復這些資料數據。很多時候, 當電腦被入侵了, 唯一的辦法是清洗系統硬盤, 然後從新安裝操作系統, 或者購買一台新的電腦。無論怎樣, 你需要你的備份來恢復你的私人資料。
- **更改密碼**: 確定要更改你所有的密碼。這不單包括你的電腦裡或移動裝置上的密碼, 而且還有所有網絡的密碼。要記得在一台安全且沒被入侵的電腦上更改你的網絡密碼。
- **防毒軟件**。如果你的防毒軟件通知你關於受感染的文件, 你可以根據它所推薦的步驟。一般這些步驟包括隔離受傳染的文件, 清洗或刪除文件。多數的防毒軟件提供鏈接的網址使你能夠了解更多關於某種感染。如果有所猶豫, 隔離受傳染的文件。如果行不通, 那就要刪除此文件。

我被入侵了, 現在怎麼辦?

- **從新安裝**。如果你不確定使用防毒軟件是否能夠清理電腦, 一個最可靠的辦法就是從新安裝電腦系統。首先, 斷開你的電腦的網絡鏈接。然後根據你的系統的生產說明書的步驟, 多數情況你需使用內裝的恢復硬盤分區來從新安裝操作系統。如果沒有恢復硬盤分區, 或已經感染或毀壞, 你需要聯絡廠家要求他們寄給你一個恢復DVD盤。不要從你的備份裡安裝操作系統。你的備份可能存在同樣的漏洞使得駭客從一開始的時候就掌握了入侵的辦法。你只有在恢復私人資料的時候才需要用你的備份。如果你的電腦已經舊了或過時了, 最簡單 (可能也是最划算) 的辦法就是購買一台新的電腦, 這樣節省了幾個小時的安裝時間。
- **專業幫助**: 如果你認為你的電腦被入侵了, 但是自己沒有把握修好, 你需要請教專業人士的幫助。比如說, 電腦被入侵之後你發覺你的備份不全或過時了, 你也許會想把重要文件好比相片, 文件或視頻從舊的電腦裡傳到新的電腦裡。可是這樣一來你會在不經意之間把惡意軟件傳送到新的電腦上, 從而感染了新的電腦。最保險到辦法是把以入侵的電腦拿到專業的技術員那裡讓他們幫你安全的恢復這些文件。

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! 備份:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! 密碼:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! 什麼是惡意軟件:	http://www.securingthehuman.org/ouch/2014#february2014
檢測邪惡 海報:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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