電腦用戶安全意識月刊

OUCH!

本期話題

- 概述
- 您已被黑客入侵的線索
- 如何應對

我被黑客攻擊, 現在該怎麼辦？

概述

我們知道您關心保護您的電腦和移動設備, 並採取措施來保護他們。但是, 無論您如何安全地使用技術, 您遲早可能被黑客入侵或“妥協”。在本月刊, 您將學習如何確定您的電腦或移動設備已經被黑客入侵, 如果這樣您就可以做些什麼。最終, 您越快發現什麼是錯的, 您回應的速度越快, 就越有可能可以減少一個網絡攻擊者可引起的傷害。

編輯嘉賓

Samantha Davison（@sam_e_davison）是在Uber安全意識和教育項目經理, 教育全球各地超過350個城市的員工。

您已被黑客入侵的線索

其實是很難確定是否被入侵, 因為往往您自己沒有單一的辦法看出來。相反, 黑客通常會留下幾個線索, 通常被稱為信號。您的系統越接近任何這些線索, 越有可能被黑客攻擊了。

- 您的防病毒程序已經觸發您的系統被感染, 特別是如果它說, 它無法刪除或隔離受感染的文件警報。
- 您瀏覽器的主頁意外改變, 或您的瀏覽器帶您到您不願意去的網站。
- 有您的電腦或設備上有您沒有創建或運行的新帳戶, 或您沒有安裝的新程序。
- 您的電腦或應用程序都在不斷崩潰, 也有未知的應用程序或奇怪的窗口彈出圖標。
- 程序請求您的授權來修改您的系統, 雖然您沒有主動安裝或更新任何應用程序。
- 當您嘗試登錄到您的系統或在線帳戶, 即使您知道您的密碼是正確的您的密碼卻不再起作用。
- 朋友問您為什麼您發送spam郵件給他們, 但您知道您從來沒有發送這些郵件。

我被黑客攻擊，現在該怎麼辦?

- 您的移動設備造成未經授權的溢價短信號碼費用。
- 您的移動設備突然不明原因有非常高的數據或電池的使用。

遲早您的電腦或設備可能會受到侵害，您發現的速度越快，越早作出回應，就越好。

如何应對

如果您認為您的電腦或設備已經被黑客入侵，您回應越早，效果越好。如果電腦或設備是由雇主提供給您或用於工作時，不要嘗試自行解決問題。您不僅可以導致弊大於利，而且您可能會摧毀可用於調查的有價值的證據。相反，將該事件馬上報告給您的雇主，通常通過聯繫您的幫助台，安全團隊或主管。如果由於某種原因，您不能聯繫您的組織，或者您擔心延遲，從網絡上斷開電腦或設備，然後把它放在睡眠，暫停或飛行模式。即使您不知道您是否已經被黑客入侵，那也最好是現在報告以防萬一。如果電腦或設備是您自己個人使用，在這裡您可以採取一些步驟。

- **更改您的密碼**: 這不僅包括改變您的電腦和移動設備的密碼，而且您所有的在線帳戶。請確保您不要使用被入侵的電腦更改密碼。相反，使用您知道是安全的不同的電腦或設備來更改密碼。
- **防病毒**。如果您的防病毒軟件通知您受感染的文件，您可以按照其建議行動。這通常可以包括隔離文件，清洗文件或刪除該文件。大多數的殺毒軟件都會有，您可以按照感染的鏈接詳細了解具體情況。如果有疑問，隔離文件。如果這是不可能的，就將其刪除。
- **重新建設**。如果您無法修復感染或要絕對確保您的系統是固定的，更安全的選擇是重建。對於電腦，遵循系統製造商的說明。在大多數情況下，這將意味著使用內置實用程序來重新安裝操作系統。如果這些實用程序丟失，損壞或感染，請與製造商聯繫尋求指導或訪問其網站。不要重新安裝從備份操作系統，他們可

我被黑客攻擊，現在該怎麼辦?

能有一個允許黑客最初獲得訪問權的安全漏洞。備份應該只用於恢復數據。對於移動設備請跟從設備製造商或服務提供的說明，這些應該是在其網站上。在許多情況下，這可能是把您的移動設備恢復到出廠默認設置一樣簡單。如果您覺得不確定重建，可以考慮使用專業的服務來幫助您。或者，如果您的電腦或設備是舊的，購買一個新的可能會更容易，甚至更便宜。最後，一旦您重建您的電腦或設備，或購買一個新的，確保它是完整的更新過，只要有可能就啟用自動更新。

- **備份**。您可以採取保護自己最重要的一步是定期備份在第一時間做準備。您備份的越勤越好。有些解決方案會每隔一小時自動備份任何新的或修改過的文件。無論哪種備份解決方案，您需要定期檢查您能夠從備份中恢復這些文件。通常，從備份中恢復您的數據是可能是被黑客攻擊後恢復的唯一途徑。
- **執法**: 如果您感到被威脅，將該事件報告給當地執法部門。

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

備份:	https://securingthehuman.sans.org/ouch/2015#august2015
口令:	https://securingthehuman.sans.org/ouch/2015#april2015
什麼是惡意軟件:	https://securingthehuman.sans.org/ouch/2016#march2016
保護您的新平板:	https://securingthehuman.sans.org/ouch/2016#january2016

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