電腦用戶安全意識月刊

OUCH!

本期話題

- 什麼是勒索軟件
- 您是否應該繳付贖金？
- 備份文件
- 進一步的保護措施

勒索軟件

什麼是勒索軟件?

客座編輯

Lenny Zeltser於NCR公司注重於維護客戶的IT運營，並在SANS研究所教授惡意軟件的戰鬥。萊尼以@lennyzeltser活躍在Twitter 上，以及在zeltser.com上寫安全博客。

勒索軟件是一種特殊類型的惡意軟件在今天整個互聯網積極蔓延，威脅摧毀受害者的文檔和其他文件。惡意軟件是一種軟件（電腦程序）用來執行惡意操作。儘管勒索軟件只是眾多不同類型的惡意軟件之一，因為它使得犯罪分子有利可圖所以已經變得非常普遍。一旦勒索軟件感染您的電腦，它將加密某些文件或者整個硬盤驅動器。然後，您的整個系統將被鎖定，或者無法訪問您的重要文件，如您的文檔或照片。該惡意軟件然後通知您，您想解密文件和恢復系統的唯一方法是支付網絡犯罪贖金（故稱為勒索）。最常見的贖金必須以某種形式的數字貨幣的支付，如比特幣。勒索軟件的傳播像許多其他類型的惡意軟件一樣。最常見的方法是通過電子郵件發送給受害者惡意電子郵件，網絡犯罪分子誘騙您打開受感染的附件或點擊，使您去到攻擊者的網站鏈接。

您是否應該繳付贖金?

這是一個艱難的問題。關鍵是越多人們支付這些罪犯，罪犯就會越有動力傳染他人。在另一方面，您可能沒有其他選擇來恢復您的文件。雖然被警告，即使您支付贖金，也不能保證您會得到您的文件備份。您是在和罪犯交涉，他們可能不解密文件，甚至如果他們為您提供解密方法以換取報酬，一但在解密過程中出錯，您的電腦可能會被感染更多的惡意軟件。

勒索軟件

備份文件

也許從一個被勒索軟件感染中恢復，並不支付贖金的最好辦法是從備份恢復您的文件。這樣一來，即使您染上勒索軟件，您可以重建或清理電腦後，恢復文件。請記住，如果您的備份可以從受感染的系統進行訪問，勒索軟件可能會刪除或加密該備份文件。因此，您的備份文件應該存放在可信的雲服務上，或者將備份存儲在並不總是連接到系統的外部驅動器。此外，一個常見的錯誤是許多人以為備份不需要測試是否能夠真正恢復。所以一定要定期測試備份是否可用，並確認在您的系統受感染後您可以恢復您需要的文件。備份是很重要的，因為它們還可以幫助您恢復您不小心刪除的文件或當硬盤驅動器崩潰時進行恢復。

勒索軟件是一種惡意軟件，一旦它感染您的電腦，會加密您的電腦上的所有文件並拒絕您訪問它們。

進一步的保護措施

保護自己免受勒索軟件感染與您防禦其他類型的惡意軟件是同樣的方式: 不要受到感染。確保您從一個值得信賴的供應商得到最新的防病毒軟件，這樣的工具，有時也被稱為反惡意軟件，旨在檢測和阻止惡意軟件。然而，反病毒無法阻止或刪除所有惡意程序。網絡犯罪分子也在不斷創新，開發新的和更複雜的惡意軟件來　避開檢測。反過來，反病毒廠商都在不斷更新自己的產品與新功能來檢測惡意軟件。在許多方面，它已成為軍備競賽，雙方都試圖智勝等。不幸的是，壞人通常是領先一步，這就是為什麼您需要確保備份您的文件，並利用這些額外的措施來保護自己:

- 網絡罪犯經常利用漏洞感染電腦或設備。您的軟件越是更新系統就越少已知漏洞使網絡罪犯感染它們。因此，請確保您的操作系統，應用程序和設備啟用自動安裝更新。

勒索軟件

- 在電腦上, 使用具有有限的權限的標準帳戶, 而不是特權帳戶, 例如 “管理員” 或 “root”。這提供了一個額外的保護: 可以阻止許多類型的惡意軟件自己安裝。
- 網絡罪犯經常誘騙人們為他們安裝惡意軟件。例如, 他們可能給您看起來合法的, 並包含一個附件或鏈接的電子郵件。也許電子郵件似乎來自您的銀行或朋友。但是, 如果您要打開附件或點擊鏈接, 您會激活能在您的系統上安裝惡意軟件的惡意代碼。如果消息產生強烈的憂患意識, 是混亂的, 似乎好得不像是真實的, 或者語法較差都可能是攻擊。可疑和常識往往是您最好的防禦。

保護自己不受到勒索, 打開電子郵件附件或點擊鏈接時保持警惕從, 確保您已經更新了防病毒軟件, 並確認您的文件定期備份並可以恢復。

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

網絡釣魚: https://securingthehuman.sans.org//ouch/2015#december2015
什麼是惡意軟件: https://securingthehuman.sans.org/ouch/2016#march2016
加密: https://securingthehuman.sans.org/ouch/2016#june2016
備份: https://securingthehuman.sans.org/ouch/2015#august2015
Microsoft文章: https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx
SANS FOR610課程 - 逆向工程惡意軟件: https://sans.org/for610

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

