電腦用戶安全意識月刊

阻止惡意軟件

概觀

當人們談論網絡安全時, 您可能已經聽說過諸如病毒, 木馬, 勒索軟件或rootkit等術語。這些是不同類型的惡意程序, 稱惡意軟件, 網絡犯罪分子用來感染電腦和設備。一旦安裝, 他們可以做任何他們想要的。了解惡意軟件是什麼, 它構成了什麼危險, 最重要的是您可以保護自己免受惡意軟件的侵害。

什麼是惡意軟件?

簡而言之, 惡意軟件是用於執行惡意操作的軟件 (一種電腦程序) 。這個術語是惡意和軟件的組合。網絡犯罪分子在您的電腦或設備上安裝惡意軟件以控制它們。一旦安裝, 惡意軟件可以使罪犯窺視您的在線活動, 竊取您的密碼或文件, 或使用您的系統攻擊他人。惡意軟件甚至可以控制您的文件, 要求您支付贖金讓他們回來。許多人認為惡意軟件只是Windows電腦的問題。不幸的是, 惡意軟件會感染任何設備, 從Mac電腦和智能手機到DVR和安全攝像頭。網絡罪犯感染的電腦和設備越多, 他們可以賺更多的錢。因此, 每個人都是一個目標, 包括您在內。

保護自己 - 阻止惡意軟件

您可能認為您所要做的就是安裝一個像殺毒軟件一樣的安全程序, 並且您可以安全地避免被感染。不幸的是, 防毒軟件無法阻止所有惡意軟件。網絡犯罪分子正在不斷開發新的更複雜的惡意軟件, 以逃避檢測。反過來, 防毒軟件供應商也在不斷更新他們的產品, 以檢測惡意軟件的新功能。在很多方面它已成為軍備競賽, 而壞人通常會領先一步。由於您無法單獨依靠防病毒, 因此您需要採取額外步驟來保護自己:

網絡犯罪分子通常利用軟件中的漏洞來感染電腦或設備。您的軟件越新，您系統的漏洞就越少，網絡犯罪分子就越難以感染它們。確保您的操作系統，應用程序，瀏覽器和瀏覽器插件以及設備始終更新且最新。確保這一點的最簡單方法是盡可能自動更新。

網絡罪犯感染電腦或移動設備的常見方式是創建假電腦程序或移動應用程序，在互聯網上發布它們，然後誘騙您下載並安裝一個。只從受信任的在線商店下載並安裝程序或應用程序。此外，遠離全新的移動應用程序，幾乎沒有正面評論，很少更新或已被少數人下載。不再使用電腦程序或移動應用程序？刪除它。

網絡犯罪分子經常欺騙人們為他們安裝惡意軟件。例如，他們可能會向您發送一封看起來合法且包含附件或鏈接的電子郵件。也許這封電子郵件似乎來自您的銀行或朋友。但是，如果要打開附加文件或單擊該鏈接，就會激活在系統上安裝惡意軟件的惡意代碼。如果一條信息產生強烈的緊迫感，或者看起來好得難以置信，那可能是一種攻擊。要提高警惕，常識往往是您最好的防守。

定期將您的系統和文件備份到基於雲的服務，或脫機存儲備份（如斷開的外部驅動器）。這會保護您的備份，以防惡意軟件嘗試加密或清除它們。備份至關重要，它們通常是從惡意軟件感染中恢復的唯一方法。

最終，防範惡意軟件的最佳方法是讓所有軟件和設備保持最新狀態，盡可能安裝可信的防病毒軟件，並對任何企圖誘騙您感染自己的系統的人警惕。當所有其他都失敗時，定期備份往往是您可以恢復的唯一方法。

客座編輯

Lenny Zeltser通過在Minerva實驗室創建終端安全產品和在SANS研究院進行教學來打擊惡意軟件。 Lenny在Twitter上以@lennyzeltser身份活躍，並在 zeltser.com上撰寫安全博客。

參考資料

勒索軟件: https://www.sans.org/u/EdI
備份: https://www.sans.org/u/EdN
阻止網絡釣魚: https://www.sans.org/u/EdS