SANS SECURITY AWARENESS

您的每月安全意識通訊

我被攻擊了嗎？

概觀

無論您多麼安全，就像開車一樣，您可能遲早會發生意外。以下我們幫助弄清楚您是否被黑客入侵的線索，如果是，那該怎麼做。您越早識別出發生了不良事件，就越有可能解決問題。

您被黑客攻擊的線索

- 您的防病毒程序會生成系統受感染的警報。確保它是您的防病毒軟件生成警報，而不是來自網站的彈出窗口，試圖欺騙您撥打號碼或安裝其他內容。不確定？打開您的防病毒程序。
- 您看到一個彈出窗口，說明您的電腦已加密，您必須支付贖金才能恢復文件。
- 您的瀏覽器帶您去到各種不想去的網站。
- 您的電腦或應用程序不斷崩潰，有未知應用程序或奇怪窗口彈出的圖標。
- 即使您知道密碼正確，您的密碼也不再有效。
- 朋友問您為什麼向他們發送垃圾郵件，而您知道從未發送過的電子郵件。
- 您的信用卡被收費或出現您從未進行過的銀行帳戶提款。

如何回應

如果您懷疑自己被攻擊了，您就越早行動越好。如果攻擊與工作有關，請不要嘗試自行解決問題，而是立即報告。如果是被黑客攻擊的個人系統或帳戶，您可以採取以下步驟

更改密碼: 這不僅包括更改電腦和移動設備上的密碼，還包括更改在線帳戶的密碼。不要使用被黑客入侵的電腦來更改密碼，使用您知道的其他安全系統。如果您有很多帳戶，請先從最重要的帳戶開始。無法記住所有密碼，請使用密碼管理器。

財務: 如果您的信用卡或任何財務帳戶出現問題，請立即致電您的銀行或信用卡公司。使用可信賴的電話號碼撥打電話，例如從銀行卡背面，財務報表或從受信任的電腦訪問其網站。此外，請考慮對您的信用檔案進行信用凍結。

防病毒: 如果您的防病毒軟件通知您受感染的文件，請按照其建議的操作進行操作。大多數防病毒軟件都會有鏈接，您可以通過這些鏈接了解有關特定感染的更多信息。

重新安裝: 如果您無法修復受感染的電腦，或者您希望確保系統安全，請重新安裝操作系統。不要從備份重新安裝，因為備份應僅用於恢復個人文件。如果您感到不確定，請考慮使用專業服務來幫助您。或者，如果您的電腦或設備較舊，則購買新電腦或設備可能會更容易。最後，一旦您重建了系統或購買了新系統，請確保它已更新並儘可能啟用自動更新。

備份: 保護自己的關鍵步驟是提前準備定期備份。許多解決方案將每天甚至每小時自動備份您的文件。無論您定期使用哪種解決方案，都要檢查是否能夠恢復這些文件。經常恢復數據備份是您從黑客中恢復的唯一方法。

執法: 如果您受到任何威脅，請將此事件報告給當地執法部門。如果您是身份盜竊的受害者並且位於美國，請訪問https://www.identitytheft.gov。

客座編輯

Johannes Ullrich博士 (@johullrich) 是SANS技術研究所研究院院長，SANS互聯網風暴中心主任和SANS研究員。他創建了DShield協作傳感器網絡，並託管了互聯網風暴中心的每日網絡安全新聞播客。

參考資料

備份: https://www.sans.org/u/JGP
密碼: https://www.sans.org/u/JGU
密碼管理員: https://www.sans.org/u/JGZ
什麼是惡意軟件: https://www.sans.org/u/JH4
信用凍結: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/