電腦用戶安全意識月刊

OUCH!

本期話題

- **社會工程**
- **檢測/阻止社會工程攻擊**
- **預防未來的攻擊**

社會工程

主要概況

一個常見的誤解人們對網絡攻擊是他們只用先進的黑客工具和技術, 闖入人們的電腦, 帳號和移動設備。這是不正確的。網絡攻擊者已經了解到, 想要竊取你的信息或入侵你的電腦, 簡單的交談並誤導你是最簡單的方法之一。本月刊中我們將學習這些類型的攻擊, 被稱為社會工程攻擊, 以及它如何工作和你可以做什麼來保護自己。

編輯嘉賓

Alissa Torres是SANS認證講師, 專業於先進的計算機取證和應急反應。她的行業經驗包括在戰壕裡掌管事件處理和工作在內部安全團隊為數字取證調查。Alissa可以在Twitter的@sibertor上聯繫到。

社會工程

社會工程學是一種心理上的攻擊, 攻擊者會誤導你做他們要你做的事。社會工程已經存在了幾千年, 欺騙活動或精讀人的想法並不新鮮。然而, 網絡攻擊已經了解到利用互聯網這種技術是非常有效的, 並且可以用於靶向百萬計的人。最簡單的方法來了解社會工程如何工作是要看看一個普通的, 現實世界的例子。

您會收到一個電話, 有人自稱是一家電腦支持的公司, 例如你的ISP或者是微軟的技術支持。來電者解釋說, 他們已經注意到, 您的電腦行為怪異, 如掃描互聯網或發送垃圾郵件, 他們認為這是感染。他們一直在負責調查這個問題, 並幫助您保護電腦。然後, 他們使用各種技術術語和帶你穿越混亂的步驟來說服你, 你的電腦被感染。

例如, 他們可能會問你要檢查, 看看是否有您的電腦上的某些文件, 並指導您如何找到他們。當你找到這些文件, 他會向你保證, 這些文件是您的電腦感染了病毒的跡象, 而實際上這些文件是在每台電腦上都能找到普通的系統文件。一旦他們欺騙你相信你的電腦被感染, 他們會迫使你進入一個網站, 並購買他們的安全軟件, 或要求你給他們遠程訪問您的電腦, 使他們能夠解決這個問題。然而, 他們所銷售的軟件實際上是一個惡意程序。如果您購買並安裝

社會工程

該軟件他們不僅騙了你感染您的電腦, 但你支付他們這樣做。如果你允許他們遠程訪問您的電腦來修復它, 實際上他們將接管以感染它。

請記住, 這樣的社會工程攻擊不限於電話;他們可以與幾乎以所有的技術出現, 包括通過電子郵件, 短信, Facebook和Twitter的消息或在線聊天進行釣魚攻擊。關鍵是要知道怎麼識別。

學習如何預防, 發現和制止社會工程攻擊是保護自己的最有效的措施之一。

檢測/停止社會工程攻擊

對抗社會工程攻擊的最簡單的方法是使用常識。如果事情看起來可疑或感覺不對, 它可能是一個攻擊。社會工程攻擊的一些常見的指標包括:

- 有人創造緊迫感。如果你覺得你有壓力做出非常迅速的決定, 是值得懷疑的。
- 有人詢問他們不應該訪問或應該知道的信息。
- 東西好得令人難以置信。一個常見的例子是, 你被告知你中獎了, 即使你從來沒有參與它。

如果您懷疑有人試圖讓你成為社交工程攻擊的受害者, 不要與他繼續溝通。如果有人給你打電話, 掛斷電話。如果是你一個人在網上聊天, 終止連接。如果是你不信任的電子郵件, 將其刪除。如果攻擊是與工作有關, 一定要立刻報告給您的幫助台或信息安全團隊。

防止未來社會工程學攻擊

幸運的是有防範措施可以採取, 以幫助防止暴露自己被未來社會工程學攻擊。

- **不要共享密碼**。沒有任何組織將與您聯繫詢問您的密碼。如果有人要求你輸入密碼, 這是一個攻擊。

社會工程

- **不要分享太多。**更多的攻擊者知道你，就越容易地找到和誤導你做他們想要的。他們甚至可以將你自己共享一段時間的小細節放在一起打造對你全面的了解。你公開分享越少，包括社會媒體網站上，商品的評論或公共論壇和郵件列表，你就越少有可能會被攻擊。

- **檢查聯繫人。**有時你可能接到你的銀行，信用卡公司，移動服務提供商或其他組織以合法的理由打來的電話。如果您有任何疑問關於信息請求是否合法，請來電人說明自己的姓名和分機號碼。然後找到可信資源公司的電話號碼，如您的信用卡背面的號碼，在您的銀行月結單的號碼，或者在公司網站上的號碼（請確保你自己在瀏覽器中鍵入URL）。當你聯繫該組織通過這種方式，你知道你是真的與他們談話。雖然這似乎是一個麻煩，但是保護您的身份和個人信息是非常值得的額外步驟。

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

電子郵件釣魚攻擊: http://www.securingthehuman.org/ouch/2013#february2013
社交網絡安全: http://www.securingthehuman.org/ouch/2013#march2013
避免詐騙: http://www.onguardonline.gov/topics/avoid-scams

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

