電腦用戶安全意識月刊

OUCH!

本期話題

- 什麼是社會工程
- 檢測/停止社會工程攻擊

社會工程學

概述

大多數人對網絡攻擊者的一個常見誤解是，他們只使用高級工具和技術來侵入人們的電腦或帳戶。這根本不是真的。網絡攻擊者已經知道，通常，竊取您的信息，破解您的帳戶或感染您的系統的最簡單的方法是簡單地欺騙您犯錯誤。在本月刊您中，您將了解這些攻擊（稱為社交工程）如何工作，以及您可以如何保護自己。

客座編輯

James Lyne（**@jameslyne**）是Sophos認證的SANS教師和全球研究主管。他用逆向工程打破了網絡罪犯的最新和最偉大的創作。他還是SANS的Metasploit（SEC580）和社會工程（SEC567）課程的作者。

什麼是社會工程

社會工程是一種心理攻擊，攻擊者欺騙您做一些您不應該做的事情。社會工程的概念不是新的，它已經存在了數千年，比如騙子都是相同的想法。使今天的技術對網絡攻擊者更有效的是，您無法看到他們，他們可以輕鬆地假裝是任何人或任何他們想要的，並針對世界各地的數百萬人，包括您。此外，社會工程攻擊可以繞過許多安全技術。理解這些攻擊如何工作並保護自己免受他們傷害的最簡單的方法是看看兩個現實世界的例子。

您會收到來自電腦支持公司，您的ISP或Microsoft技術支持人員的電話。調用者解釋您的電腦正在主動掃描互聯網，他們認為它被感染，並已被任命幫助您保護您的電腦。他們然後使用各種技術術語，並帶您通過混亂的步驟，說服您的電腦被感染。例如，他們可能會要求您檢查電腦上是否有某些文件，並引導您完成如何找到它們。當您找到這些文件時，調用者確保這些文件證明您的電腦被感染，當實際上這些文件是在世界上幾乎每個電腦上找到的常見系統文件。一旦他們欺騙您相信您的電腦被感染，他們迫使您購買他們的安全軟件或

社會工程學

讓他們遠程訪問您的電腦, 以便他們可以解決它。然而, 他們銷售的軟件實際上是一個惡意程序。如果您購買和安裝它, 不僅會感染您的電腦, 您還付了款讓他們去做。如果您讓他們遠程訪問您的電腦, 他們將把它完全操控, 竊取您的數據或出售它。

常識是您在識別和阻止大多數社會工程攻擊時最強大的防禦。

另一個例子是名為CEO　騙局的電子郵件攻擊, 這通常發生在工作。這是當網絡攻擊者在線搜索您的組織, 並確定您的老闆或同事的名字。攻擊者然後製作一個假裝來自該人的電子郵件, 並將電子郵件發送給您。電子郵件迫切要求您採取行動, 例如進行電匯或發送敏感的員工信息。這些電子郵件通常假裝緊急需要您繞過標準安全程序, 例如他們可能會要求您將高度敏感的信息發送到個人@　gmail.com帳戶。使這樣的有針對性的攻擊如此危險是網絡攻擊者在這之前充分做過他們的研究。此外, 防病毒或防火牆等安全技術無法檢測或停止這些攻擊, 因為沒有涉及惡意軟件或惡意鏈接。

請記住, 像這樣的社會工程攻擊不限於電話或電子郵件;他們可以以任何形式發生, 包括您的手機上的短信, 通過社交媒體, 甚至親自面對。關鍵是要知道要注意什麼, 您是您自己最好的防禦。

檢測/停止社會工程攻擊

幸運的是, 停止這樣的攻擊比您想像中更簡單 - 常識是您最好的防禦。如果有些東西看起來很可疑, 或者覺得不對勁, 那可能是攻擊。社會工程攻擊的最常見線索包括:

- 有人創造了巨大的緊迫感, 他們試圖欺騙您犯錯誤。

社會工程學

- 有人要求他們不應該訪問或應該知道的信息, 例如您的帳號。
- 有人要求您輸入密碼, 沒有合法的機構會要求您提供密碼。
- 有人強迫您繞過或忽略您期望在工作中遵循的安全過程或過程。
- 好到難以相信。例如, 通知您贏得彩票或iPad, 即使您從來沒有買彩票。
- 您收到來自朋友或同事的一封奇怪的電子郵件, 其中的聲音聽起來不像真的是他們。網絡攻擊者可能已經入侵他們的帳戶, 並試圖欺騙您。為了保護自己, 請使用其他通訊方式 (例如親自見面或通過電話) 與您的朋友聯繫, 以驗證此類請求。

如果您懷疑有人試圖欺騙或愚弄您, 不要再與該人溝通。如果攻擊與工作相關, 請務必立即向幫助台或信息安全團隊報告。記住, 常識通常是您最好的防禦。

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
CEO欺詐:	https://securingthehuman.sans.org/ouch/2016#july2016
勒索軟件:	https://securingthehuman.sans.org/ouch/2016#august2016
OUCH檔案:	https://securingthehuman.sans.org/ouch/archives

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