SANS SECURITY AWARENESS

OUCH!

全民資訊安全意識月刊

CEO變臉詐騙 / BEC

什麼是CEO變臉詐騙 / BEC?

網路犯罪份子目前發展出一種被稱為CEO變臉詐騙或商業電子郵件入侵 (BEC) 的電子郵件攻擊手法。他們利用特定的電子郵件進行攻擊, 誘使受害者做出錯誤的行動。在大多數情況下, 他們的目的是騙取金錢。這種攻擊手法危險之處在於發動攻擊之前, 駭客會先研究對象的相關資料。事實上, 就連安全技術工具也很難阻止這些攻擊, 因為不會有受感染電子郵件附件或惡意連結可被檢測。以下是變臉攻擊的操作手法:

駭客會先在網路上調查詐騙對象及其人際關係的相關資料。假設您是他們的目標, 首先他們會查出您公司老闆或是房地產經紀人是誰, 然後製作一封電子郵件, 假裝是這些人當中的一員並寄電子郵件給您。電子郵件內容通常表現相當緊急, 並要求立即採取行動, 例如處理發票、更改付款人或是回覆機敏文件。這類詐騙郵件能夠生效的原因乃是在急迫情況下逼您倉促行事。以下是兩個攻擊成功的例子:

匯款詐騙: 網路犯罪份子的目標是錢。首先他們會調查您任職的公司, 例如查出誰在付款部門工作或誰負責資金轉帳; 然後, 他們發送假的電子郵件給這些人, 並且偽裝成是他們的老闆或高階主管。電子郵件內容告知有緊急情況, 必須立即將錢轉移到新的銀行帳戶。負責人員受到郵件內容情境逼迫下而犯下錯誤, 事實上錢是匯到了網路犯罪份子的帳戶。

稅務詐騙: 網路犯罪份子會將他人的個資用於稅務詐騙。獲得個人資料的快速方法之一是竊取公司所有員工的資料。犯罪份子首先會調查誰在人力資源部門工作, 然後向這些人發送假的電子郵件, 冒充成高階主管或者是法務部門的人。電子郵件內容會塑造出緊急的情境, 並要求必須立即提供所有員工的稅務資訊。人力資源部門人員以為這些機敏文件是發送給主管, 實際上他們正在將資料發送給駭客。

如何保護自己

那麼, 可以做些什麼來保護自己呢? 具備防詐騙常識就是最好的自保之道。以下舉出一些慣用詐騙手法有哪些破綻:

- 電子郵件內容非常短且緊急 (通常只有幾句話) , 且簽名檔顯示電子郵件是從行動裝置發送出來的。
- 電子郵件內容帶有強烈的急迫感, 促使您省略或跳過公司的相關政策要求。提醒您, 即使電子郵件看似來自公司老闆甚至CEO, 也務必要遵循與工作相關的政策和程序, 。
- 電子郵件內容雖與工作相關, 但使用個人電子郵件地址, 例如@ gmail.com或@ hotmail.com。
- 電子郵件看起來像是主管、同事或供應商寄送的, 但內容表達的語氣似乎不像是他們。
- 電子郵件內容為付款指示, 但是與以前既有的做法不一樣, 例如要求立即向其他銀行帳戶付款。

在工作時, 如果您覺得自己已經成為詐騙者下手的目標, 請立即停止與其的所有互動, 並向主管報告。如果您是在家中被鎖定詐騙, 或不幸已經匯出款項, 請立即通知您的銀行, 然後報警。

德欣寰宇為台灣專業資訊安全顧問公司。我們為客戶提供全方位安全整合解決方案。請至官方網站 http://www.tsc-tech.com/或臉書@tsctech了解更多訊息。

客座編輯

Don Cavender以前曾是FBI幹員, 在數位鑑識和網路犯罪領域擁有超過22年經驗。他目前擔任美國華府的BEC協調員, 專精網路犯罪組織。同時, 也提供數位鑑識及網路調查方面的訓練及專業研究。可以在以下地方找到他的資料:

@don_cavender https://www.linkedin.com/in/donald-cavender

資源

社交工程	https://www.sans.org/u/HE3
網路釣魚:	https://www.sans.org/u/HE8
防堵惡意軟體:	https://www.sans.org/u/HEd
鎖定登入:	https://www.sans.org/u/HEi

編輯委員會: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | 翻譯群: 黃意雯、宋亞倫、顧君毅、孫權劭、葉力維、莊銘輝