OUCH!2024年12月

OUCH!

SANS SECURITY AWARENESS

您的每月安全意識月刊

揭露陰影：網路犯罪分子如何竊取您的密碼

數位惡夢：麗莎的意外暴露

麗莎是一位富有創意的平面設計師，她的大部分生活都在網路上度過。她透過各種應用程式和網站管理銀行事務、購物和社交互動。有一天，她注意到她的銀行帳戶有一些奇怪的提款——她從未購買過的商品，來自她從未造訪過的商店。然後，她的社交媒體帳戶開始發布促銷奇怪產品和服務的垃圾訊息，朋友們也告知收到來自她的異常電子郵件。

當麗莎意識到自己已經失去了對數位身份的控制時，恐慌油然而生。她的個人照片被洩露，私密對話也被曝光。客戶開始質疑她的可靠性，她的聲譽也受到損害。在諮詢了網路安全專家後，麗莎發現她的密碼已經遭到洩漏。網路犯罪分子已經獲得她最敏感帳戶的存取權，逐步瓦解了她的數位世界。揮之不去的問題是：這到底是怎麼發生的？

網路犯罪分子的卑鄙手法：五種常見方式

網路威脅者採取各種技術來竊取密碼。以下是他們可能像對麗莎一樣獲得您的密碼的五種常見方式：

1. **社交工程攻擊**

   社交工程是指攻擊者假裝成您熟悉或信任的人事物，並欺騙您做一些不應該做的事情。他們會發送看似合法的電子郵件或訊息，通常會製造出強烈的緊迫感、恐懼或好奇心。

   *事情是這樣發生的：*麗莎收到了一封看起來像是來自她銀行的電子郵件，有完整的官方標誌和品牌設計。該電子郵件聲稱她的帳戶有可疑活動，並催促她點擊連結以驗證她的身份。該連結導向一個假網站，當她輸入登入憑證時，該網站便捕捉了她的資料。

2. **惡意軟體**

   惡意軟體是旨在感染電腦的惡意程式。一旦感染，網路犯罪分子便可以為所欲為。鍵盤側錄器（有時稱為*竊資程式*）是一種惡意軟體，能記錄在設備上輸入的每個按鍵，包括您的登入資訊、密碼和其他敏感資料。

   *事情是這樣發生的：*麗莎下載了她認為是合法的字型套件，以用於她的設計工作。其中隱藏著一個鍵盤側錄器，並自動安裝在她的電腦上。隨著時間過去，它記錄了她多個帳戶的登入憑證，並將這些資料發送回攻擊者。

3. **暴力破解攻擊**

   在暴力破解攻擊中，網路犯罪分子使用自動化工具嘗試無數的密碼組合，直到猜中正確的密碼。面對這種攻擊時，弱密碼特別脆弱。*事情是這樣發生的：*麗莎的許多帳號使用了簡單的密碼，例如「lisa2020」。攻擊者使用軟體系統性地嘗試常見密碼，輕易地破解了她的帳號。

4. **資料洩露**

當一個網站或服務遭到駭客攻擊時，可能會影響儲存在伺服器上的所有用戶帳號。如果某人的多個帳號使用相同的密碼，當其中一個帳號的密碼被洩漏後，攻擊者就可以使用這個密碼來存取受害者的其他帳號。

*事情是這樣發生的：*麗莎使用的一個受歡迎的社交媒體平台發生了資料洩露事件。由於她在其他地方也使用了相同的密碼，攻擊者利用洩漏的憑證存取了她的其他帳號。

5. **購買憑證**

網路犯罪分子可以輕易地在網路上購買您的密碼，通常是在暗網。某些網路犯罪分子專門竊取受害者的密碼，使用我們之前討論過的任何方法。然後，他們將竊取的密碼儲存起來並轉售給其他網路犯罪分子。

*事情是這樣發生的：*一名網路犯罪分子決定在週末盡可能賺取金錢，因此他們進入暗網，購買了超過100,000個已被竊取的帳號及其完整密碼。麗莎的其中一個帳號就在名單上。

您能採行的三個重要步驟

幸運的是，透過採取三個簡單的步驟，您可以大幅提升保護您的帳號和數位生活的安全性。

1. 請為每個帳號使用長且獨特的密碼。我們建議使用密詞，這是一種由多個單詞組成的長密碼。
2. 使用密碼管理工具來安全地儲存並管理所有這些密碼。
3. 儘可能為最重要的線上帳號啟用多因子驗證 (MFA)。

客座編輯

Lekshmi Nair 是一位資深的網路安全領導者，擁有22年豐富的資訊安全諮詢與網路安全策略經驗。她目前擔任 BlackDuck Software 的應用程式安全諮詢高級總監。她是 WiCyS India 的創辦人兼主席。

資源

虛幻之聲：防禦語音複製攻擊：
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltf73b6a1c7e1fd5f5/66c48f6a33f9a594427a8721/ouch!_chinese_(Traditional_Taiwan)_september_2024_voice_cloning.pdf
簡訊攻擊：一個簡訊釣魚的故事：
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt2b3111ca5cb21032/666c534951f6563f52b72ab6/ouch!_july_2024_Chinese_(Traditional_Taiwan)_spot_and_stop_messaging_attacks.pdf
網路攻擊鎖定您的三大方式：
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltfa51a67cd5c4491b/6619c4124906453ecb0394d5/ouch!_may_2024_chinese_(Traditional_Taiwan)_top_three_ways_cyber_attackers_target_you.pdf
密詞之力：
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt848a55a198b7bb59/655518f625f479dc94d44a8b/ouch!_december_2023_chinese_(Traditional_Taiwan)_power_of_the_passphrase.pdf
密碼管理器：
https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt8141844941b24b17/64b1b6661511874c6d038eb8/ouch!_august_2023_chinese_(Traditional_Taiwan)_power_of_password_managers.pdf

由社群翻譯：宋亞倫 德欣寰宇科技股份有限公司

OUCH!是由美國系統網路安全研究協會（SANS Security Awareness）發行，遵從創意公用授權條款4.0版(Creative Commons BY-NC-ND 4.0)。在不更改本刊物內容或出售的前提下，您能夠自由分享及發佈此月刊。編輯委員會：Walter Scrivens、Phil Hoffman、Alan Waggoner、 Leslie Ridout、Princess Young。