SANS SECURITY AWARENESS

上網肉搜自己

概述

您很可能聽過保護您的隱私和您透過網路分享的資訊非常重要。為了證明這一點，我們將嘗試一些新的方法，我們將向您示範如何研究您自身並找出有關您的公開資訊。這個過程被稱為OSINT（Open Source Intelligence，公開來源情資的一種酷炫簡稱），意思是透過研究網路上公開的資訊，以了解電腦IP地址、公司甚至某個人，比如說您自己的更多情報。請記住，網路攻擊者也使用這些相同的工具和技術。攻擊者了解的越多，他們就越能夠啟動目標式攻擊。這個概念已存在多年，但最新的線上工具使其更加簡單易行。

如何搜尋資訊

您無法在一個網站上就找到所有資訊。您應該做的是從一個網站開始，了解一些細節，然後使用這些細節搜尋並從其他網站得知更多。您可以結合並比較結果，建立關於目標的概要文件或檔案。搜索引擎是一個好的起點，像是Google、Bing或DuckDuckGo。每個搜尋引擎都有不同關於您的資訊索引，因此請使用多個搜尋引擎搜索。首先輸入您的名字，然後根據所謂的搜尋運算子展開搜索。搜尋運算子是您添加到搜尋中的特殊符號或字元，可以更好地定義您要查找的內容。如果您有一個菜市場名，這一點尤為重要，您可能需要添加更多資訊，例如您電子郵件地址或居住城鎮。請看結尾參考資料中有關搜尋運算子和進階搜尋技巧的更多資訊。例子包括：

⚠

- **姓名>在網路上找到有關此人的資訊**
- **姓名@>搜尋和此人相關的電子郵件地址**
- **姓名filetype:doc>任何包含此姓名的Word檔案**

有一些網站致力於了解人們。試試其中一個網站，看看您的公開資訊有那些。請記住，這些網站不一定準確，也可能限定使用區域。您可能需要搜索多個網站以驗證您找到的資訊。

- https://pipl.com
- https://cubib.com
- https://familytreenow.com

最後，還有許多其他網站可供您搜尋以了解更多資訊，例如Google圖片、Google地圖和社群媒體網站等等。有關您可以用來了解自己的所有不同網站的互動式列表，我們建議您使用https://osintframework.com。

為什麼要上網肉搜自己?

1. **了解其他人或組織在網路上蒐集、發佈或分享了哪些與您有關的內容（教堂、學校、體育俱樂部或其他在地社區網站）**
2. **了解這些資源同樣可供其他任何人使用，包括可以使用該資訊鎖定您的網路罪犯。要心存懷疑，例如，如果您接到某人打來的緊急電話，對方聲稱是您的銀行，不能只是因為他們知道您的一些基本資料就證明了電話來自您的銀行。請禮貌地掛斷，然後用一個已知的可信號碼打電話給您的銀行，以確認他們的身份。電子郵件也一樣，信件中有一些關於您的已知事實並不代表這封信是正常的。**
3. **考慮您公開分享的內容以及資訊可能對您、您的家人或您的雇主產生的影響。**

客座編輯

Nico Dekens (@dutch_osintguy) 擅長OSINT (公開來源情資)。他的日常生活環繞著網路情資蒐集分析。 Nico是財富500強公司和政府部門的OSINT、物聯網和營運安全等主題的國際講師。

參考資源

社交工程攻擊:	https://www.sans.org/u/LW6
安全使用社群媒體的最佳提示:	https://www.sans.org/u/LWb
搜尋運算子:	https://support.google.com/websearch/answer/2466433
OSINT Framework:	https://osintframework.com/
SANS OSINT Course SEC487:	https://www.sans.org/u/LWZ

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