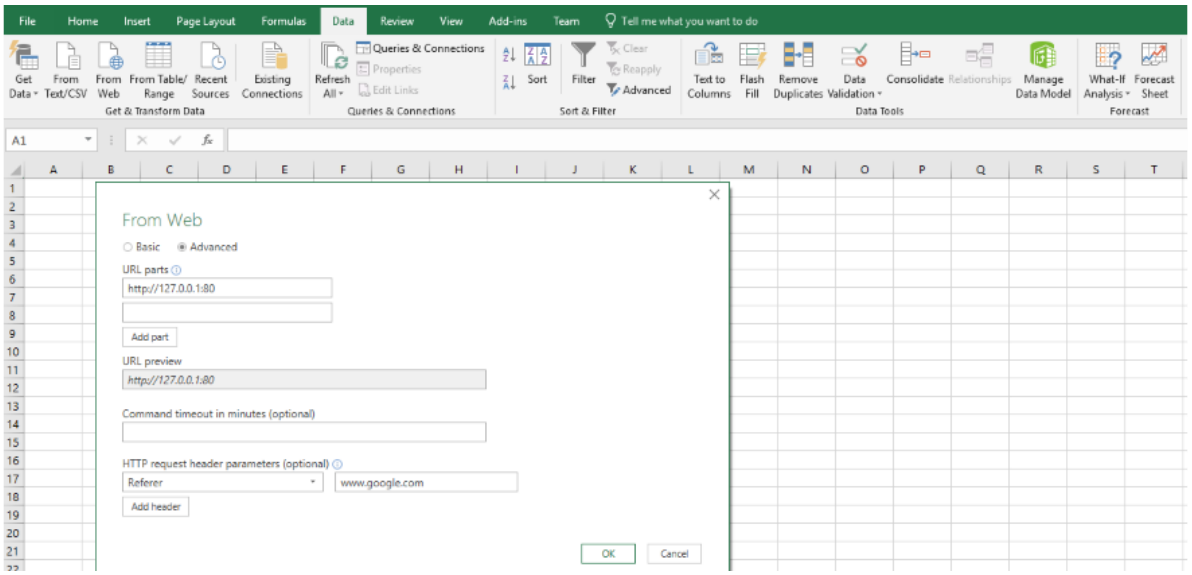
資安業者警告微軟 Excel 中的 Power Query 功能過於強大，反而為駭客帶來許多潛在攻擊機會，例如在試算表開啟時植入或執行惡意程式

文/陳曉莉 | 2019-06-28 發表



利用 Power Query 執行惡意攻擊示意圖（圖片來源：Mimecast ）

資安業者 Mimecast Threat Center 近日指出，微軟 Excel 試算表中的 Power Query，可能遭到駭客開採而自遠端植入惡意程式，不過，微軟並未將它當成安全漏洞，也不打算修補，而是提出了基於安全設定的解決辦法。

Power Query 為一資料連結技術，可用來搜尋、連結、整合或調整不同的資料來源以滿足使用者的分析需求，當連結這些來源時，資料即可被存入或動態載入，該功能同時出現在 Excel 與 Power BI 上。

Mimecast 安全研究團隊負責人 Ofir Shlomo 指出，藉由 Power Query，駭客可在某個來源中嵌入一個惡意內容，並在試算表開啟時載入該內容，以用來植入或執行惡意程式，屬於遠端動態資料交換（Dynamic Data Exchange，DDE）攻擊。

Shlomo 表示，Power Query 具備豐富的控制能力，可在遞送任何酬載（payload）前辨識沙箱或受害者機器，有機會讓駭客取得潛在的預先載入或預先開採控制能力，在將惡意酬載傳送給受害者時，還能讓檔案看起來無害。

Mimecast 並不確定這是 Power Query 功能或是安全漏洞，但在知會微軟之後，微軟並不打算修補，而是提供了解決方案，包括利用群組原則（Group Policy）或是 Office 的信任中心（Office Trust center）來阻擋外部的檔案連結。

不過，Shlomo 依然認為 Power Query 過於強大而帶來許多潛在的攻擊機會，像是本地端權限擴張、DDE 攻擊或遠端程式執行等。Mimecast 也展示如何以一個外部的伺服器來代管惡意酬載，當 Microsoft Excel 2016 用戶以 Power Query 請求該網頁時，載入惡意內容。

另一方面，過去微軟也曾提供有關 Office 應用程式中處理動態資料交換時的安全建議，Mimecast 呼籲所有 Excel 用戶應導入相關的安全設定，以避免成為網路攻擊的受害者。

資料來源:iThome