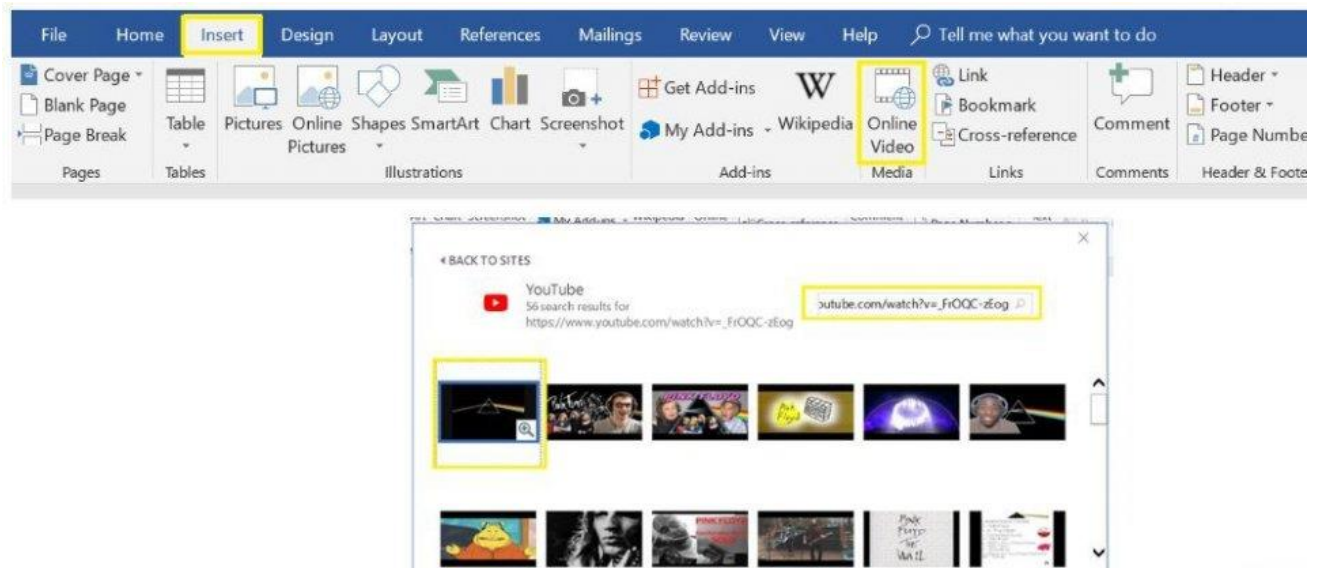


當心! 插入 YouTube 影片的 Word 文件可能讓惡意程式上身

駭客可以建立一個插入線上影音的 Word 文件，例如 YouTube，竄改 Word 文件夾中的 document.xml 檔案的參考，再誘導受害者開啟文件，就會呼叫 IE 執行嵌入的檔案，感染勒索軟體或木馬。

文/[陳曉莉](#) | 2018-10-29 發表



以色列資安業者 [Cymulate](#) 上周揭露一新的攻擊手法，可以利用微軟 Word 中的線上影音 (Online Video) 功能來展開惡意程式攻擊。只是微軟並不認為這是個安全漏洞。

根據 Cymulate 技術長 Avihai Ben-Yossef 所描述的攻擊場景，駭客在建立一個 Word 文件之後，可透過插入 (Insert) 功能嵌入線上影音，如任何的 YouTube 影片，將其存檔後再展開 (Unpack) 該文件，找到 Word 文件夾中的 document.xml 檔案，在 embeddedHtml 參數中將 YouTube 的 iframe 程式碼置換成任何 HTML 或 Javascript 程式並加以儲存。

當駭客透過網釣攻擊誘導受害者開啟該文件時，就會呼叫 IE 來執行所嵌入的檔案，而它也許已被置換成勒索或木馬程式。

Ben-Yossef 表示，該漏洞可能影響所有 Office 2016 及舊版 Office 用戶，要重製此一攻擊行動完全不需要特別的配置，而且使用者在開啟此一 Word 文件時，也不會接收到任何的安全通知。

Cymulate 已經在 3 個月前知會微軟，但 Threatpost 引述微軟的回應表示，這並不是個安全漏洞，該產品正確地依照既有的設計解讀了 HTML，跟其它類似的產品一樣。Ben-Yossef 則建議企業封鎖那些內含嵌入影片的 Word 文件。

資料來源：iThome