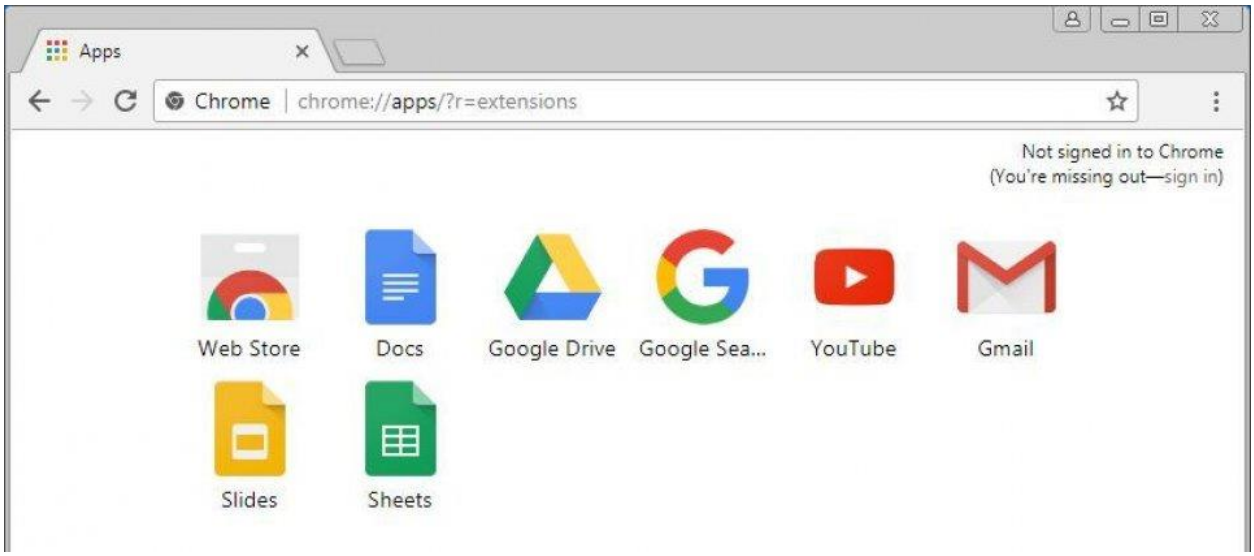
當心！惡意 Chrome、Firefox 擴充程式強迫安裝，而且狡猾地不給用戶移除

Malwarebytes 發現在 Chrome、Firefox 上出現惡意擴充程式，以強迫安裝的方式植入用戶的電腦中，而且以相當狡猾地以種種手法不讓用戶輕易移除，經揭露後 Chrome 的惡意擴充程式已被下架。

文/林妍溱 | 2018-01-22 發表



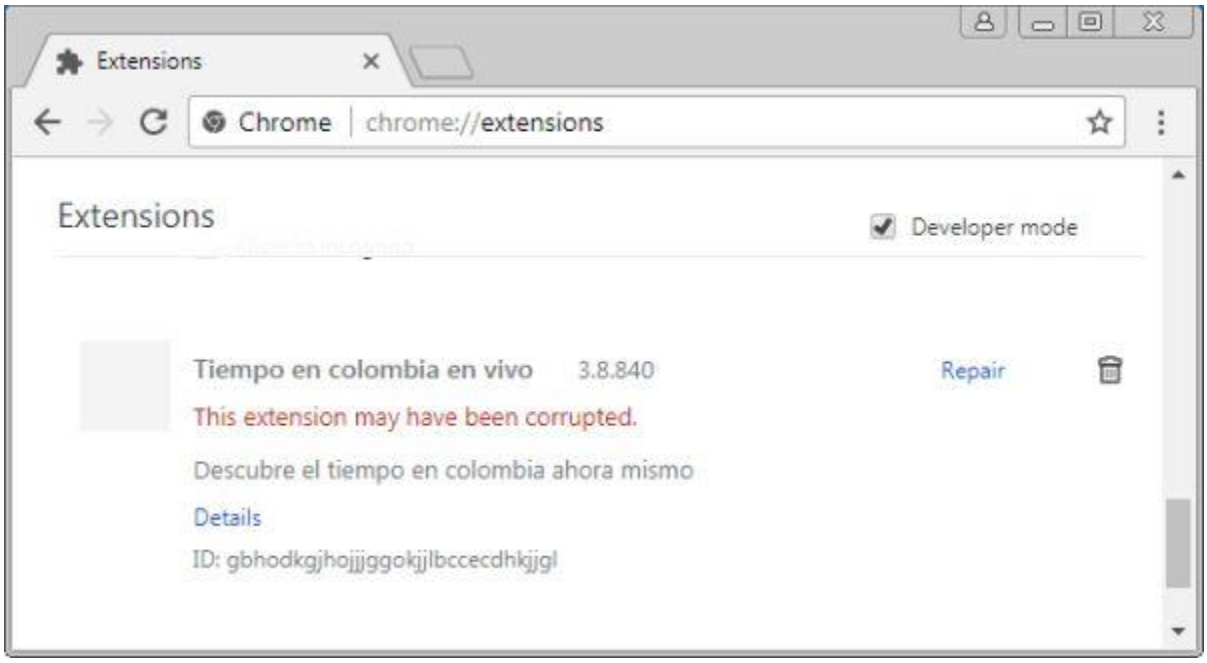
瀏覽器擴充程式已然成為新的安全問題。安全公司 Malwarebytes 分別發現 Chrome 與 Firefox 有惡意擴充程式安裝後竟會使用詭計不讓用戶移除。

在 Chrome 上的惡意擴充程式稱為 Tiempo en Colombia en vivo。它是該公司 2016 年發現強迫安裝 Chrome 擴充程式的一種手法而流傳。在這種手法下，網站被植入一種惡意 JavaScript 程式，會在用戶不小心造訪網站時跳出對話框，要求使用者如果要離開網站就必須安裝擴充程式。一般人會按「取消」，這時它會再顯示「避免本頁再產生其他對話框」的對話框。通常使用者會按下「OK」。不過這會讓用戶被導向全螢幕模式，並看見自己正要安裝的擴充程式。

Tiempo en Colombia en vivo 一旦被安裝到電腦上，它會使 Chrome 出現異常行為。例如研究人員 Pieter Arntz 在測試機器上發現它會自動點擊十多部 YouTube 影片，似乎要衝刺點閱率。

但當用戶想要移除它時會發現難上加難。首先，它不讓用戶連結 chrome://extensions/，即可一覽 Chrome 擴充程式並移除的頁面，而是導向 chrome://apps/?r=extensions。在這個頁面上自然找不到這個惡意擴充程式。封鎖 Chrome 中的 JavaScript 也沒有用，因此這個方法只適用於外部網頁，對本機上的網頁無效。而在 Chrome 下執行「–disable-extensions」指令也沒用，因為 Chrome 會顯示它沒有擴充程式。

唯一方法是修改擴充程式資料匣中的 1499654451774.js 檔名。此後重新啟動 Chrome 即會在 chrome://extensions/顯示所有擴充程式，包括 Tiempo en Colombia en vivo，但因為其 JavaScript 被重新命名，因此會顯示該檔案已損毀。但這時即可將之刪除。（來源：Malwarebytes）



Malwarebytes 研究人員也在 Firefox 發現有類似手法的擴充程式，名為 PUP.Optional.FFHelperProtection。但它是以網站上的廣告輪播程式推送出 Firefox 手動更新的詐騙廣告，誘騙使用者下載。安裝後它會在用戶搜尋擴充程式頁時，以 background.js 尋找 URL 的字串，然後將之關閉，讓使用者想移除也找不到。

不過這個擴充程式比較容易對付。只要在啟動 Firefox 時按著 Shift 鍵，按下「以安全模式啟動」的選項。在安全模式的 Firefox 下，所有擴充程式都會現形，讓使用者得以手動移除。而且如果 Firefox 因為 JavaScript，對話框一再跳出而動彈不得的話，只要利用「工作管理員」即可關閉 Firefox。

Tiempo en Colombia en vivo 在上周四都可在 Chrome Web Store 上下載。Malwarebytes 公佈並由 Ars Technica 報導後，Google 已經將之移除。PUP.Optional.FFHelperProtection 則並未在 Firefox 擴充程式商店中發現。

由於這兩款惡意擴充程式可能是利用強迫安裝法安裝到用戶端，有可能被趁虛而入。因此安全公司建議不要下載來路不明的擴充程式，並使用廣告封鎖工具。最好方法是詳細閱讀任何擴充程式的使用條款。

這是最新發現的惡意 Chrome 擴充程式。近年來 Chrome 擴充程式常被駭客用來散佈惡意廣告程式。本月又有資安業者分別發現

Chrome Web Store 上有 Chrome 擴充程式被植入採礦程式或點擊詐騙程式，消息曝光後 Google 才將之移除。