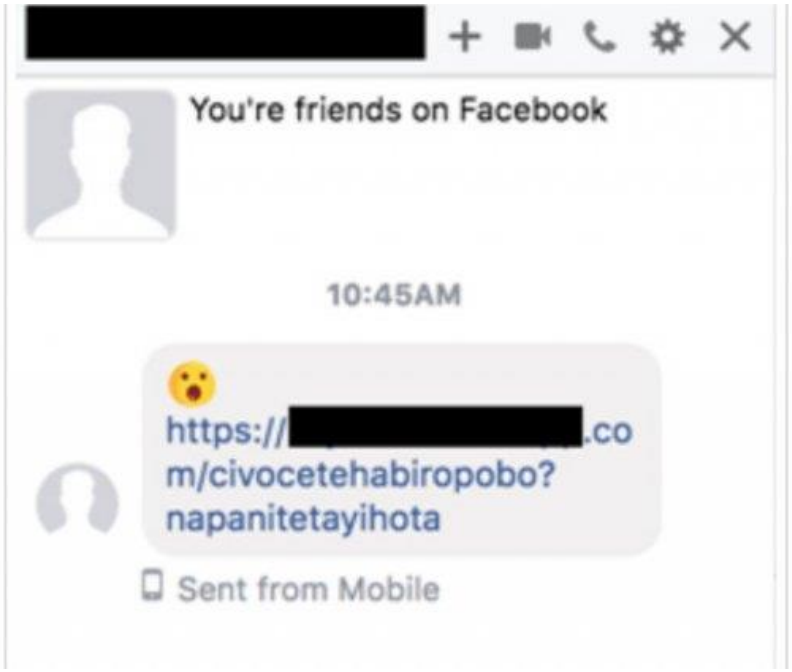
趨勢：惡意程式專門利用臉書 Messenger 感染 Chrome 用戶，直指加密貨幣而來

文/陳曉莉 | 2018-05-01 發表



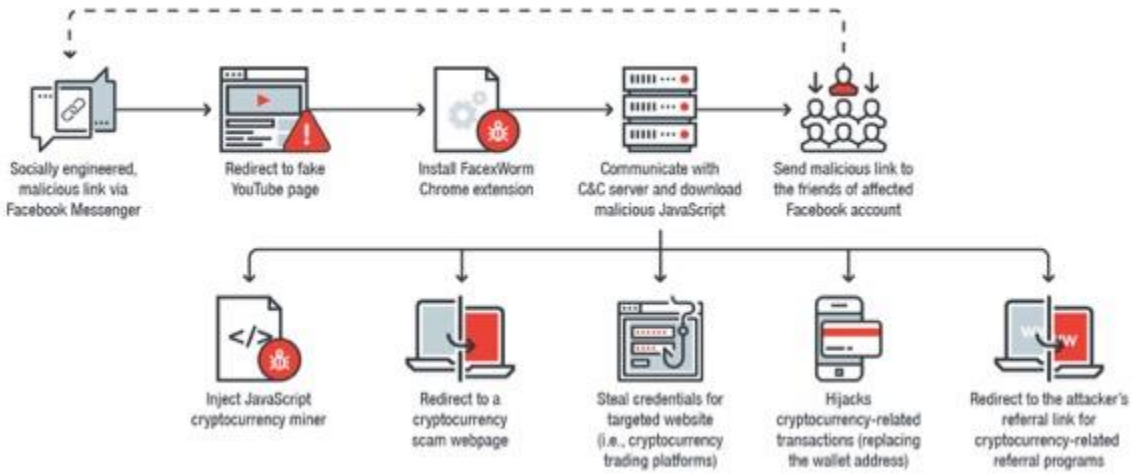
FacexWorm 利用 Facebook Messenger 散布，它化身為 YouTube 連結，要求使用者安裝 Chrome 擴充程式以播放影片，並取得存取及變更使用者所造訪網站的資料權限。

趨勢科技本周披露了一個專門藉由 Facebook Messenger 進行散布，且主要感染 Chrome 瀏覽器用戶的 FacexWorm 惡意程式，該惡意程式鎖定的目標為近來盛行的加密貨幣，包括竊取用戶加密貨幣憑證、進行加密貨幣詐騙、誘導用戶造訪遭植入採礦程式的網頁，以及挾持加密貨幣的交易等，功能非常完善。

FacexWorm 被植入於許多 Chrome 擴充程式中，在去年 8 月就被發現，但趨勢在今年 4 月上旬發現它更活躍了，同時出現在德國、突尼西亞、日本、台灣、南韓與西班牙等市場。

FacexWorm 採用社交工程手法並利用 Facebook Messenger 進行散布，它化身為 YouTube 頁面的連結，要求使用者安裝 Chrome 擴充程式以播放影片，並取得存取及變更使用者所造訪網站之資料的權限。一旦使用者按下同意，FacexWorm 就會自 C&C 伺服器下載其它惡意程式，並開啟 Facebook，伺機取得用戶的友人名單，再傳遞偽造的 YouTube 影片連結，擴大感染範圍。

感染手法：



該惡意程式只鎖定 Chrome 瀏覽器，萬一遇到其它瀏覽器，使用者即會被導向廣告網頁。

成功進駐 Chrome 瀏覽器之後，只要使用者開啟一個新網頁，FacexWorm 就會與 C&C 伺服器交流並展開各式的惡意行動，涵蓋竊取 Google、MyMonero 與 Coinhive 等服務的憑證；或是在使用者所造訪的網頁上注入採礦程式；若使用者開啟的是加密貨幣的交易網頁，FacexWorm 就會把使用者的錢包位址置換成自己的；也會竄改使用者的路徑以讓駭客獲得特定網站的推薦獎勵。

此外，尚若使用者造訪了駭客所指定的 52 個加密貨幣交易平台，FacexWorm 即會直接把使用者導向詐騙網頁，宣稱使用者只要匯出

0.5~10 個以太幣至駭客的帳號，以協助該帳號的驗證，便能獲得 10 倍的回饋。

趨勢表示，在接到該公司的通報前，Google 已經移除了一些與 FacexWorm 有關的擴充程式。至於臉書也已得知 FacexWorm 的行動，亦已封鎖了被駭帳號的散布行為。趨勢奉勸使用者應培養良好的安全習慣，注意陌生或可疑的訊息，分享前要三思，且於社交網站上採用較嚴格的隱私設定。

資料來源：iThome