

駭客挾持 Chromecast 等眾

多連網裝置以播放任意

YouTube 影片

兩名駭客發動名為 CastHack 的攻擊行動，開採 Chromecast、路由器的安全漏洞，以劫持 Chromecast 及連網電視播放特定的 YouTube 影片。

文/[陳曉莉](#) | 2019-01-03 發表

代號為 Hacker Giraffe 與 J3ws3r 的兩名駭客在本周針對 Chromecast、Google Home 及智慧電視等連網裝置發動攻擊，迄今已挾持逾 6 萬台相關裝置以播放來自 YouTube 頻道 PewDiePie 的影片。

這兩名駭客將此一攻擊行動命名為 CastHack，宣稱是開採了 Chromecast 及路由器的安全漏洞，以強迫 Chromecast 與連網電視播放他們所選擇的任何 YouTube 影片。

駭客的入侵點為「通用隨插即用」（UPnP）協定，該協定允許家庭網路或企業網路中的各種裝置能夠無縫連結，也會將內部網路的連結

埠轉送到全球網路上，而使得 Chromecast 或其它連網裝置曝露於公開網路上。

因此，Hacker Giraffe 與 J3ws3r 所挾持的裝置不只是 Chromecast，還包括 Google Home 與智慧電視，不只已強迫 6.5 萬台裝置播放影片，還替逾 8,200 台裝置更換了名稱。例如有一名用戶在 Reddit 上抱怨他原本在看的電視節目每 20 分鐘會自動切換成 PewDiePie 的影片，影片中即出現#ChromeCastHack 的字樣。

除了播放 PewDiePie 的影片之外，駭客也在電視上秀出警告訊息，指出使用者的 Chromecast 及智慧電視已曝露於公開網路上，還外洩了機密資料。這些機密資料包含這些裝置所連結的 Wi-Fi 網路、所配對的藍牙裝置、連網時間或是所設定的鬧鐘等。

Hacker Giraffe 與 J3ws3r 表示，此一攻擊除了允許遠端駭客於裝置上播放任何媒體內容之外，還能變更裝置名稱，將裝置回復成出廠預設值，或是重新啟動裝置，也能強迫裝置忘掉所有的 Wi-Fi 網路，或是強迫裝置與新的藍牙喇叭、Wi-Fi 熱點配對。

這兩名駭客也提供了暫時修補方式—關閉路由器上的 UPnP，以及禁止轉送 8008/8443/8009 等傳輸埠。

Hacker Giraffe 與 J3ws3r 說他們的攻擊行動只是為了警告漏洞威脅，並沒有任何惡意的企圖，還說日前挾持 5 萬台印表機，以讓它們列印出 PewDiePie 頻道廣告的攻擊行動也是他們的傑作。

資料來源：iThome