

Mozilla 與 Tor 修補瀏覽器上 同一個零時差漏洞

Mozilla 與 Tor 分別修補了 Firefox 及 Tor Browser 瀏覽器上同一個零時差漏洞，駭客先將惡意程式嵌入兒童色情網站，當使用者以 Tor Browser 造訪該站時就會遭到感染，蒐集用戶的 IP 與 MAC 位址，從而取得其真實身份。

Mozilla 與 Tor 專案 (Tor Project) 在本周三 (11/30) 相繼更新了旗下的 Firefox 與 Tor Browser 瀏覽器，以修補已遭開採的零時差漏洞。

這兩個組織基本上所修補的是同一個安全漏洞，有鑑於 Tor Browser 是基於開放源碼的 Firefox 所打造，因而遭到波及；更新版的 Tor Browser 即是採用修補過後的 Firefox。

已現身的攻擊程式鎖定的 Tor Browser，它利用 Firefox 上的安全漏洞來蒐集 Tor Browser 用戶的 IP 與 MAC 位址，藉以得到 Tor Browser 用戶的真實身分。駭客先將惡意程式嵌入知名的兒童色情網站 Giftbox，感染以 Tor Browser 造訪的使用者電腦，再將系統 IP 及 MAC 位址傳遞至遠端伺服器。

該漏洞同時影響 Windows、macOS 與 Linux 平台，雖然攻擊程式目前僅鎖定 Windows 平台，尚未發現針對 macOS 或 Linux 的攻擊程式，然而不論是 Mozilla 或 Tor 都呼籲所有系統的用戶皆應儘速更新。

外界猜測此一攻擊程式可能是由 FBI 或其他執法機構所建置，因為它運作的方式與 FBI 在 2013 年時用來辨識 Tor 用戶的網路調查技術一致。Mozilla 認為，假設該程式果真是由執法機構所開發，那麼它現在已允許任何人用來攻擊 Firefox 用戶，更證明了政府的駭客手法將對整體網路造成威脅。

資料來源：iThome