PlugX(Win.Trojan.Xamtrav)資安事件說明及後門清除建議

PlugX(Win.Trojan.Xamtrav)簡介

PlugX(又稱為 Win.Trojan.Xamtrav)是駭客廣為運用的後門程式。據目前了解，此次事件是一個被命名為 Winnti Group 的組織所為。他們在過去曾經攻擊上百個遊戲公司，竊取遊戲原始碼、在遊戲檔案植入惡意程式、竊取使用者密碼等行為。

此次 Garena 公司遭受針對性攻擊，目前已知有流亡黯道(Path of Exile)及英雄聯盟(League of Legends)兩款遊戲被植入此惡意程式。

簡易檢測

若您在過去四個月(2014/09~2014/12)曾經從 Garena 公司官網下載主程式並執行安裝，您很有可能是此次資安事件的受害者。

請檢查電腦是否有以下兩個檔案，如果有，確認您是此次事件受害者。

C:\Windows\System32\NtUserEX.dll

C:\Windows\System32\NtUserEX.dat

後門清除建議措施

一、建議使用趨勢線上清除工具，也可以使用 Garena 公司提供一年免費的 F-Secure 防毒軟體。

趨勢線上清除工具下載與安裝說明，請參考以下連結：

http://esupport.trendmicro.com/solution/zh-TW/1107253.aspx

二、更新最新版 Garena 遊戲。

Garena 公司於 2014/12/29 已發佈更新檔，只要更新 12/29 後的檔案即可修正問題執行檔。也可以完整移除舊有程式，從官網下載最新版的安裝程式安裝。

三、更換密碼。

為確保使用者帳號的安全性，建議玩家定期更新密碼，避免有心人士盜用。

四、啟用免費的兩步驟驗證。

可以啟用 Garena 兩步驟驗證，以加強對帳號密碼的保護。

詳細資訊請參考 Garena 公司官網說明：

http://lol.garena.tw/news/news_info.php?nid=2532