Flashback 木馬簡介

一、 攻擊概述：

一支存在於 MAC 上的木馬程式。一開始出現的時候只是被偽裝成 Flash Player 的安裝程式，不過現在已經出現了變種，可以透過瀏覽惡意網站時經由 Mac OS X 的 Java 漏洞感染。另外 Flashback 不是指單一的惡意軟體，而是一個木馬家族，還有許多的後門程式。

二、 攻擊平台：Mac OS X

三、 攻擊手法介紹：

1. 當用戶被重定向至帶有惡意程式碼的頁面時，會載入一段包含漏洞的 Java 小程式。這個漏洞在被感染機器上釋放一個可執行檔，用來與遠端伺服器連接並執行其他惡意行為。因為這些網站往往會打著下載或更新一個“新版本的 Flash Player”的幌子來欺騙用戶下載，並且會請求使用者輸入管理員密碼。因此這個病毒被命名為“Flashback”。
2. 病毒第一次運行時會搜索特定路徑是否含有以下防毒軟體元件：

   /Library/Little Snitch
   /Developer/Applications/Xcode.app/Contents/MacOS/Xcode
   /Applications/VirusBarrier X6.app
   /Applications/iAntiVirus/iAntiVirus.app

/Applications/avast!.app
/Applications/ClamXav.app
/Applications/HTTPScoop.app
/Applications/Packet Peeper.app

如果沒有發現，後門程式會通過特殊的途徑生成一個控制伺服器列表，將安裝成功的通知內容發送至攻擊者的伺服器，並且根據伺服器清單進行連續性的查詢。

3. 接下來，主機會被接到一個殭屍網路(Botnet)，攻擊者在主機上安裝額外的惡意模組，某些模組偽造搜尋引擎結果，提供錯誤的搜索結果，並利用“點擊欺詐”產生利潤。
4. 除此之外，攻擊者也會上傳其他元件，例如資料竊取，垃圾郵件(SPAM)等模組。這個惡意軟體會使用負載均衡技術，動態切換伺服器。每個被控制端將被賦予唯一的 ID 並發送至控制伺服器。

四、 檢測方法：

檢查您的 Mac 是否已經感染 Flashback 木馬，可以經由 F-Secure 提供的檢查法。

1. 首先請先打開 Mac OS X 的終端機後，輸入 defaults read /Applications/Safari.app/Contents/Info LSEnvironment
2. 如果回應的訊息內有出現「The domain/default pair of (/Appplications/Safari.app/Contents/Info,LSEnvironment) does not exist」的話。

3. 接著輸入 defaults read ~/.MacOSX/environment DYLD_INSERT_LIBRARIES
4. 如果回應中包含「The domain/default pair of (/Users/joe/.MacOSX/environment,DYLD_INSERT_LIBRARIES) does not exist」的話，就表示您的 Mac 並未受到感染。

五、 防護方法：

- 該病毒利用的 Java 漏洞有：

  CVE-2008-5353
  CVE-2011-3544
  CVE-2012-0507

- 盡早更新 Mac 發布的更新檔以及 Flash Player、Java 的更新。

- 使用防毒軟體偵測並刪除 OSX_FLASHBCK.AB、OSX_FLASHBCK.A、OSX_FLASHBCK.DL、OSX_FLASHBCK.IC

六、 參考資料：

1. http://whiteappleer.tw/2012/04/06/is-your-mac-infected-by-the-flashback-trojan-affecting-600000-macs/
2. http://whiteappleer.tw/2012/05/15/apple-updates-mac-os-x-105-leopard-with-flashback-removal-tool-flash-player-disabler/
3. http://blog.trendmicro.com.tw/?p=1284&%E6%BC%8F%E6%B4%9E%E6%94%BB%E6%93%8A/osx_flashbck%E6%89%93%E7%A0%B4mac-os%E4%B8%8D%E6%98%93%E4%B8%AD%E6%AF%92%E7%9A%84%E8%AA%AA%E6%B3%95%E4%B8%8B%E4%B8%80%E6%B3%A2%E5%8F%AF%E8%83%BD%E6%98%AF%E7%B6%B2%E8%B7%AF%E9%8A%80

%E8%A1%8C%E6%9C%A8

4. http://www.ithome.com.tw/itadm/article.php?c=73125