一、弱點知識庫

＊Adobe 發布 Flash Player 安全更新

說明	更新修補的 Flash Player 漏洞，是由於 Memory corruption 的方式讓攻擊者可以對電腦執行任意代碼。攻擊者可能利用這種漏洞攻擊方式，取得受害者電腦控制權並執行任意代碼，進一步能安裝程式，檢視、變更或刪除資料，或建立具有完整使用者權限的新帳戶。
影響	該漏洞可能導致攻擊者取得系統控制權限。
影響系統	-Adobe Flash Player Desktop Runtime 18.0.0.232 and earlier -Adobe Flash Player Extended Support Release 18.0.0.232 and earlier -Adobe Flash Player for Google Chrome 18.0.0.233 and earlier -Adobe Flash Player for Microsoft Edge and Internet Explorer 11 18.0.0.232 and earlier -Adobe Flash Player for Internet Explorer 10 and 11 18.0.0.232 and earlier -Adobe Flash Player for Linux 11.2.202.508 and earlier -AIR Desktop Runtime 18.0.0.199 and earlier -AIR SDK 18.0.0.199 and earlier -AIR SDK & Compiler 18.0.0.180 and earlier -AIR for Android 18.0.0.143 and earlier
建議解決方法	1. 建議使用者應儘速更新至最新版本。 2. 相關網站： https://helpx.adobe.com/security/products/flash-player/apsb15-23.html

＊XcodeGhost

說明	Xcode 為蘋果的程式開發環境，提供程式碼編輯器、資產目錄編輯器、iOS 模擬器，及除錯工具等。XcodeGhost 是首個 OS X 中的編譯病毒，相關的病毒碼被重新包裝至某些版本的 Xcode 安裝版本中，而這些含有病毒的 Xcode 則被上傳到中國 OS X 與 iOS 開發人員經常使用的百度雲端分享服務上，導致許多原本合法的中國 iOS 程式也夾帶了病毒。
影響	攻擊者可以取得受害者裝置內的資訊，包括裝置的名稱、系統語言和國家、網路特性（包括受害者儲存的 WiFi 密碼），甚至可以遙控某裝置打開某個連結、製造假的設定讓用戶按下去、甚至直接讀寫用戶儲存在手機的資料，包括剪貼簿的文字、儲存在某應用程式內的密碼等等。
影響系統	受到影響的 App 程式眾多，而截至 9 月 20 日下午的通報，受感染 app 數量為 1078 款。知名度較高的部分 App 如：微信、網易雲音樂、滴滴打車、高德地圖、12306、同花順、中信銀行動卡空間、簡書等。涉及包括即時通訊軟體、地圖應用甚至金融服務產品。
建議解決方法	1.如果安裝了受感染的 App，請盡速移除或更新到最新狀態。 2.開發者避免到第三方網站下載工具。 3.參考資料： http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/

二、惡意程式分析報告

(一)前言

誘捕網路（Honeynet）即是一個可以誘捕駭客活動與行為、收集各項威脅的方式的網路。Honeynet是一種屬於高互動式的誘捕系統群，主要是由多個有缺陷、不具營運價值的誘捕系統(Honeypot)所構成，藉由模擬真實的系統行為和網路服務回應，不僅可以誘使駭客進行攻擊，還可捕捉並紀錄攻擊手法和系統行為的改變，並將蒐集到的攻擊資訊回饋給相關人員進行分析並改善網路防禦的方法。

本分析報告即是針對『教育部教育學術資訊安全監控中心(A-SOC)暨殭屍電腦(Botnet)防禦機制建置計畫』所佈署之Honeynet誘捕網路所蒐集到之惡意程式進行分析說明。

(二)惡意程式分析

1.惡意程式基本資料

(1)單一識別碼(Hash值)

◆MD5：71c0568c4f6e22baded5d150c2854bff

◆SHA-1：838bcc63cf97da85ff4fcddc771d7877fef280b1

(2)惡意程式檔案大小：98,304 bytes

(3)各防毒軟體定義名稱：

◆ ESET-NOD32：VBA/TrojanDownloader.Agent.AEC

◆ Kaspersky：Trojan-Downloader.VBS.Agent.auc

◆ TrendMicro：W2KM_DRIDEX.XDC

◆ McAfee：W97M/Downloader.aoe

2.惡意程式行為分析

(1) 新增檔案

這隻惡意程式會在受害者的系統磁區中新增以下檔案：

◆ C:\Documents and Settings\User\Local Settings\Temporary Internet Files\Content.IE5\4XEJWTA3\98kj6[1].exe

◆ C:\Documents and Settings\User\Local Settings\Temporary Internet Files\Content.IE5\0XQV8DI3\84.246.226[1].htm

◆ C:\Documents and Settings\User\Local Settings\Temporary Internet Files\Content.IE5\UXAF8DAF\84.246.226[1].htm

(2) 修改系統啟動清單

◆ 該惡意程式在被執行後，會透過修改以下機碼，修改受害主機啟動清單

● HKEY_USERS\\S-1-5-21-1547161642-507921405-839522115-1004\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon

(3) 資訊蒐集

該惡意程式會蒐集系統資訊，包含系統BIOS時間，MachineGuid...等，並存取本機的瀏覽器瀏覽歷史紀錄，來蒐集被害主

機上的網頁瀏覽行為。

(4)與外部主機進行聯絡

該惡意程式在成功感染受害主機後，會從外部主機下載檔案，資訊如下：

◆ 網域名稱：performatic.xf.cz
- ✓ IP：88.86.117.154
- ✓ 國家：捷克
- ✓ 連線位置：http://performatic.xf.cz/fw43t2d/98kj6.exe

◆ 網域名稱：www.download.windowsupdate.com
- ✓ IP：96.6.45.114
- ✓ 國家：美國
- ✓ 連線位置：
  http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
  http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootseq.txt

(三) 提升本機安全性防護

1.安裝防毒軟體並定期更新病毒碼

建議電腦使用者必須要安裝防毒軟體並定期病毒碼，避免網路威脅發生。

2. 開啟本機防火牆並定期安裝系統更新

開啟微軟系統內建之系統更新功能，定期針對系統重大更新以及安全性更新檔進行安裝，避免系統暴露在攻擊的威脅之下。

3.惡意程式移除工具

若使用者的電腦系統不慎遭到此惡意程式感染而無法正常運作，請下載各大防毒軟體廠商所釋出之惡意程式移除工具，以進行病毒清除程序。以下網址可供參考：

(1)Microsoft Safety Scanner,官方網站：
http://www.microsoft.com/security/scanner/zh-tw/default.aspx

(2)TrendMicro System Cleaner,官方網站：
http://downloadcenter.trendmicro.com/index.php?regs=TW

(3)Norton Rescue Tool,官方網
http://tw.norton.com/free-tools-trial/promo