一、弱點知識庫

＊Adobe 發佈 Flash Player 安全更新

說明	Adobe 發佈多個 Flash Player 安全漏洞，部分漏洞是由於整數溢出或記憶體損壞缺陷，攻擊者可能利用漏洞取得系統控制權限，進而達到攻擊者目的。
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 20.0.0.306 and earlier -Adobe Flash Player Extended Support Release 18.0.0.329 and earlier -Adobe Flash Player for Google Chrome 20.0.0.306 and earlier -Adobe Flash Player for Microsoft Edge and Internet Explorer 11 20.0.0.306 and earlier -Adobe Flash Player for Internet Explorer 11 20.0.0.306 and earlier -Adobe Flash Player for Linux 11.2.202.569 and earlier -AIR Desktop Runtime 20.0.0.260 and earlier -AIR SDK 20.0.0.260 and earlier -AIR SDK & Compiler 20.0.0.260 and earlier -AIR for Android 20.0.0.233 and earlier
建議解決方法	建議使用者應儘速修補。 https://helpx.adobe.com/security/products/flash-player/apsb16-08.html

＊SSL.RSA.Temporary.Key.Security.Bypass

說明	在 OpenSSL 及 Microsoft Windows 產品中，SSL/TLS 加密協定存在中間人攻擊(man in the middle attack) 破解加密金鑰弱點。利用中間人攻擊修改 ClientHello 與 ServerHello 封包，將 RSA 或 DHE（Diffie-Hellman Ephemeral）金鑰加密演算法降階為較弱的 EXPORT 演算法，受害主機被破解加密金鑰的風險將因而提高。
影響	攻擊者便可擷取、還原加密封包並取得機敏內容。。
影響系統	-OpenSSL 1.0.1k、1.0.0p、0.9.8zd 及更早版本 -Windows Server 2003、2008(R2)、2012(R2) -Windows Vista、7、8、8.1、RT、RT 8.1。
建議解決方法	1.建議儘快更新軟體版本以修補漏洞並評估是否關閉 EXPORT 演算法，採用安全性較高的 ECDHE（Elliptic Curve Diffie-Hellman Ephemeral）演算法。 2.相關參考資料網站： https://www.openssl.org/news/newslog.html https://technet.microsoft.com/library/security/3046015

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

- 單一識別碼(Hash 值)
  - MD5：ca83b8c7bea221c630dcbc766e0d9e14
  - SHA-1：345df0f422711274cae57ef1da351e66447b2065
- 惡意程式檔案大小： 870,232 bytes
- 各防毒軟體定義名稱：
  - Avast：NSIS:Adware-IE [PUP]
  - BitDefender：Adware.Nieguide.C
  - Symantec：Trojan.Gen.2
  - TrendMicro：TROJ_GEN.R03FC0ED216

(2)惡意程式行為分析

- 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:\DOCUME~1\User\LOCALS~1\Temp\nsx2.tmp\KillProcDLL.dll
  - C:\DOCUME~1\User\LOCALS~1\Temp\nsx2.tmp\Ischeck.dll
  - C:\DOCUME~1\User\LOCALS~1\Temp\nsx2.tmp\installoption.ini
  - C:\DOCUME~1\User\LOCALS~1\Temp\nsx2.tmp\NSISPromotionEx.ini
  - C:\DOCUME~1\User\LOCALS~1\Temp\nsx2.tmp\DLLWaitForKillProgram.dll
  - C:\DOCUME~1\User\LOCALS~1\Temp\nsx2.tmp\FILEDownPlug.dll
  - C:\DOCUME~1\User\LOCALS~1\Temp\nsx2.tmp\installoption.ini
- 竊取使用者的個人資料，該惡意程式在感染主機後，會修改受害電腦的瀏覽器安全設定，增加未經授權的網域；此外，該惡意程式亦會存取使用者的網路瀏覽紀錄
  - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
  - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
  - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
  - HKEY_CURRENT_USER\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
  - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings

- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\\Domains\vaccinescan.co.kr

➢ 與外部主機聯絡：該惡意程式在成功感染受害主機後，會對外部主機發起 HTTP 連線，資訊如下:

A. 網域名稱：update.vaccinescan.co.kr
   - ✓ IP：無
   - ✓ 國家：韓國

(3) 提升本機安全性防護

➢ 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。

➢ 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。

➢ 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：

- Microsoft Safety Scanner,官方網站：http://www.microsoft.com/security/scanner/zh-tw/default.aspx
- TrendMicro System Cleaner,官方網站：http://downloadcenter.trendmicro.com/index.php?regs=TW
- Norton Rescue Tool,官方網站：http://tw.norton.com/free-tools-trial/promo