一、弱點知識庫

＊Adobe Flash Zero-Day

說明	Adobe Flash Player (CVE-2015-7645)這漏洞攻擊，是以魚叉式網路釣魚郵件，透過全球所注目的國際事件為主旨來吸引收件人開啟郵件。成功的攻擊可讓攻擊者取得受害者系統的控制權。
影響	該漏洞可能導致攻擊者取得系統控制權限。
影響系統	-Windows 和 Macintosh 上 Adobe Flash Player 19.0.0.207 版本以及之前的版本。 -Adobe Flash Player 延伸支援 18.0.0.252 版本以及 18.x 之前的版本。 -Adobe Flash Player 11.2.202.535 版本以及 11.x 之前的版本。
解決方法建議	1.升級至最新版本。 2.Windows 專用 Flash Player 11.2.x 或更高版本使用者，或是 Macintosh 專用 Flash Player 11.3.x 或更高版本使用者，若有選取「允許 Adobe 安裝更新」選項，將會自動收到更新。並未啟用「允許 Adobe 安裝更新」選項的使用者，可在提示時透過產品內的更新機制安裝更新。 3.相關網站： https://helpx.adobe.com/security/products/flash-player/apsb15-27.html https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7645

＊Back to 28: Grub 2 Authentication Zero-Day

說明	Grub 2 存在一項虧失（integer underflow）漏洞，編號 CVE-2015-8370。 當按足 28 次 Backspace 時就會使記憶體錯誤，攻擊者便可以進入 Grub rescue shell 來存取電腦資料和安裝惡意軟體等。
影響	攻擊者可以提高權限、複製磁碟資訊、安裝 rootkit、或是摧毀包括 Grub 在內的任何資料，即使磁碟加密也可能遭到覆寫，導致系統無法作業。
影響系統	98 版到 2.02 版 Grub 2 都存在這項漏洞。
解決方法建議	1.相關網站： ● http://hmarco.org/bugs/CVE-2015-8370-Grub2-authentication-bypass.html ● https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-8370 2.更新修補程式資訊： ● Grub 2：http://hmarco.org/bugs/patches/0001-Fix-CVE-2015-8370-Grub2-user-pass-vulnerability.patch ● Ubuntu：https://lists.ubuntu.com/archives/ubuntu-security-announce/2015-December/003218.html ● Red Hat：https://rhn.redhat.com/errata/RHSA-2015-2623.html ● Debian：https://security-tracker.debian.org/tracker/CVE-2015-8370 ● Fedora：https://lists.fedoraproject.org/pipermail/package-announce/2015-December/173703.html

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：cf991952063458eeca50ef7043366ca3
  - SHA-1：24c5f7f27a743f81f82c294245eaebf90c794d63
- 惡意程式檔案大小： 1,213 bytes
- 各防毒軟體定義名稱：
  - BitDefender：Generic.Banker.Delf.5CDE5A71
  - Avira：TR/Spy.Banker.6967808
  - Symantec：Infostealer.Bancos!gen
  - McAfee：PWS-Banker.gen.ad

(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:\WINDOWS\Help\tours02\sstub.txt
  - C:\WINDOWS\system32\drivers\bvxzq.sys
  - C:\cleanup.exe
  - C:\cleanup.bat
  - C:\WINDOWS\Help\tours02\omc.exe
  - C:\ebdlcnpu.txt
  - C:\zip.exe
- 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_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- 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：www.rubenspaiva.com.br
    - ✓ IP：162.144.115.49

- ✓ 國家：美國
- ✓ 連線位置：
  http://www.rubenspaiva.com.br/demo/empresa/Pastas/group/post.php

(3) 提昇本機安全性防護

- ➢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