一、弱點知識庫

＊JavaScript 的開發平台 Node.js 與 io.js 存有弱點

說明	網路應用程式若使用 V8 JavaScript Engine 的 Node.js 或 io.js，存在字串轉換的弱點，攻擊者可能使用該弱點造成阻斷服務攻擊(DoS)。
影響	攻擊者可能利用 JavaScript 的開發平台 Node.js 與 io.js 存有的弱點發動 DoS 攻擊。
影響系統	node.js-v0.12.6、io.js-v2.2.3、io.js-v1.8.3。
建議解決方法	1. 建議使用者應儘速更新。 2. 更新相關網站： http://blog.nodejs.org/2015/07/03/node-v0-12-6-stable/ https://github.com/nodejs/io.js/blob/v2.3.3/CHANGELOG.md https://github.com/nodejs/io.js/blob/v1.8.3/CHANGELOG.md 3. 相關參考資料： https://www.us-cert.gov/ncas/current-activity/2015/07/06/Security-Updates-Nodejs-and-iojs

＊Android 2.2 版至 5.1.1_r4 版存在整數溢位漏洞

說明	在 Android 處理多種常見媒體格式的媒體函式庫"Stagefright"，存在遠端程式碼執行漏洞，包含多個整數溢位問題(overflow 與 downflow)的記憶體錯誤。
影響	攻擊者只需要知道用戶手機號碼，寄發多媒體簡訊（MMS）惡意的多媒體檔案即可入侵用戶手機，並遠端執行程式碼。
影響系統	Android 2.2 (Froyo) 至 Android 5.1.1_r4 (Lollipop)。
建議解決方法	1. 建議使用者應儘速到手機官網更新 Android 至 5.1.1_r5 版本。 2. 相關參考資料： http://www.kb.cert.org/vuls/id/924951

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)

- ◆MD5：0280c4d548d0bc6d44f6fc05a1482bd7
- ◆SHA-1：2cff27edba6ce3ace4039ee2fe00da2b7143804f
- ◆SHA-2:173604e753fd719fefb5e427a053ecf94749e29e1b1f852a175f0f518d6898a7

(2)惡意程式檔案大小：420,401bytes

(3)各防毒軟體定義名稱：

- ◆ BitDefender：Trojan.GenericKD.2542345
- ◆ Kaspersky：Trojan-PSW.Win32.Fareit.bbgt
- ◆ McAfee：RDN/Generic PWS.y!b2l
- ◆ Sophos：Troj/Fareit-GO

2.惡意程式行為分析

(1)修改受害主機的檔案系統

此惡意程式在感染主機後，會新增以下2個檔案：

- ◆ C:\DOCUME~1\User\LOCALS~1\Temp\specification.scr
- ◆ C:\DOCUME~1\User\LOCALS~1\Temp\957236.bat

(2)嘗試修改本機機碼並自動安裝惡意程式

- ◆ 該惡意程式在被執行後，會透過修改以下機碼，促使受害主機安裝該惡意程式自動產生之螢幕保護程式(specification.scr)：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-1547161642-507921405-839522115-1004\Installer\Assemblies\C:|DOCUME~1|User|LOCALS~1|Temp|specification.scr
- ◆ HKEY_CURRENT_USER\Software\Microsoft\Installer\Assemblies\C:|DOCUME~1|User|LOCALS~1|Temp|specification.scr
- ◆ HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Assemblies\C:|DOCUME~1|User|LOCALS~1|Temp|specification.scr

(3)與外部主機進行聯絡

該惡意程式在成功感染受害主機後，會對外部主機發起連線，並嘗試傳送HTTP封包：

- 網域名稱：skylink.hostei.com
- IP：31.170.160.249
- 國家：美國
- 連線位置：http://skylink.hostei.com/pony/gate.php

(三)系統更新與病毒移除

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且定期進行病毒碼更新，避免受到病毒侵害。

2.開啟本機的防火牆

建議電腦使用者使用微軟系統內建之防火牆或是其他信賴第三方的防火牆來過濾電腦的網路通訊，及早發現不明的網路通訊，降低其所造成的風險。

3.定期安裝系統安全性更新檔

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。

4.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