一、弱點知識庫

＊Dell 電腦預載憑證軟體 eDellRoot 存在安全性弱點

說明	Dell 電腦預載一項名為「eDellRoot」的 SSL 認證憑證，主要供原廠進行裝置故障回報時的機制。攻擊者可以利用此機制漏洞入侵 Dell 筆電，並且竊取使用者機敏資料。
影響	攻擊者可以利用此漏洞竊取使用者機敏資料。
影響系統	-XPS 13 -XPS 15 -Precision M4800 -Inspiron 系列桌上電腦 -Inspiron 系列 5000 筆電
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：http://www.kb.cert.org/vuls/id/870761

＊Symantec Endpoint Protection(SEP) 12.1 存有弱點

說明	Symantec Endpoint Protection(SEP) 12.1 存在多個弱點，遠端攻擊者可以利用弱點提升權限、執行任意程式碼，取得系統控制權。
影響	遠端攻擊者可利用此弱點，執行任意程式。
影響系統	-Symantec Endpoint Protection Manager 12.1-RU6-MP3 之前版本 -Symantec Endpoint Protection Clients 12.1-RU6-MP3 之前版本
建議解決方法	1. 建議使用者應儘速更新至最新版本。 2. 更新至 SEP 12.1-RU6-MP3 以後的版本。 3. 相關網站： http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20151109_00

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)

◆MD5：894fe9a77ec411f0303085e69e280b24

◆SHA-1：8164010831b884629647e7b57ad98652ef8ad502

(2)惡意程式檔案大小：731,152 bytes

(3)各防毒軟體定義名稱：

◆ BitDefender：Trojan.GenericKD.2853166

◆ Avira：TR/Crypt.Xpack.313663

◆ TrendMicro：BKDR_AN.EC7B81CD

◆ McAfee：Ransom-CWall.c!B00664DBE479

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:\myapp.exe

◆ C:\DOCUME~1\User\LOCALS~1\Temp\Documento198432.exe

(2) 該惡意程式在被執行後，會對主機的檔案系統加密，迫使受害者支付費用:

(3) 與外部主機聯絡：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:

A. 網域名稱：zsn5qtrgfpu4tmpg.onion.gq
- ✓ IP：194.42.118.104　國家：荷蘭

B. 主機位置：
- ✓ IP：171.25.193.9　國家：瑞典

C. 主機位置：
- ✓ IP：76.73.17.194　國家：美國

(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