一、弱點知識庫

＊IE 重大漏洞，攻擊者可以取得與目前使用者相同的使用者權限

說明	攻擊者可以針對這個經由 Internet Explorer 引起的弱點來設計並架設蓄意製作的網站，然後引誘使用者檢視該網站。攻擊者也可能利用受侵害的網站，以及接受或存放使用者提供之內容或廣告的網站 (透過新增蓄意製作以利用此弱點的內容)。如果使目前用者以系統管理的使用者權限登入，成功利用此弱點的攻擊者可以取得受影響系統的完整控制權。攻擊者接下來將能安裝程式，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	遠端攻擊者可以取得與目前使用者相同的使用者權限。
影響系統	Windows 用戶端上的 Internet Explorer 7 (IE 7)、Internet Explorer 8 (IE 8)、Internet Explorer 9 (IE 9)、Internet Explorer 10 (IE 10) 和 Internet Explorer 11 (IE 11)。
建議解決方法	1.檢查防火牆紀錄：查看記錄是否有外界對貴單位內部 IP 之異常連線。 2.如發現為非授權的連線，建議將該 IP 於防火牆阻擋。 3.建議使用者應儘速更新。 相關資料： https://technet.microsoft.com/zh-tw/library/security/MS15-093

＊聯想電腦 BIOS 中 Lenovo Service Engine (LSE)存在安全性弱點

說明	Lenovo 在個人電腦的 BIOS 韌體中，利用微軟的 Windows 機制嵌入了聯想服務引擎（Lenovo Service Engine, LSE），LSE 除了會下載用來強化 PC 效能的 OneKey Optimizer 程式外，也會回傳系統資訊至聯想伺服器上。LSE 可能會遭到濫用，允許駭客展開緩衝區溢位攻擊，或是連至聯想的測試伺服器。
影響	該漏洞可能導致遠端取得系統控制權。
影響系統	Lenovo 個人電腦包含數十款的桌機與筆電，製造日期自 2014 年 10 月 23 日至今年的 4 月 10 日，所執行的作業系統為 Windows 7、Windows 8 或 Windows 8.1。
解決方法建議	1.自行關閉 LSE 功能。 2.下載可移除 LSE 的程式。 相關資料： https://support.lenovo.com/us/en/product_security/lse_bios_notebook https://support.lenovo.com/us/en/product_security/lse_bios_desktop

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)

◆MD5：05c9bf5f1c9e139038adacf9b222efc1

◆SHA-1：4125b24f8e1142718130dd2af42045a343c5557b

(2)惡意程式檔案大小：1,945,600bytes

(3)各防毒軟體定義名稱：

◆ BitDefender：Gen:Variant.Symmi.55913

◆ Kaspersky：UDS:DangerousObject.Multi.Generic

◆ McAfee：TROJ_GEN.R00TC0DI215

◆ Sophos：Mal/VMProtBad-A

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\Application Data\dressabhis.exe

◆ C:\Documents and Settings\User\Local Settings\Application Data\nstantlyleks.exe

(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_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

(3) 具有反砂箱偵測能力

藉由偵測Bios以及主機軟硬體資訊來判斷是否處在砂箱分析環境中。

(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：rotabr53.com
- IP：192.169.90.108
- 國家：美國
- 連線位置：http://rotabr53.com/magazins2/network_1.zip

(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