一、弱點知識庫

＊Apache Struts Dynamic Method Invocation Bug Lets Remote Users Execute Arbitrary Code on the Target System

說明	針對 Apache 的 Struts 2.3.20 至 Struts 2.3.28(2.3.20.2、2.3.24.2 除外)版本，攻擊者可透過 DefaultAction.java 的 invokeAction 弱點，將惡意攻擊程式碼夾帶於 Request 中，允許攻擊者遠端執行任意程式碼
影響	遠端攻擊者可利用此弱點，執行任意程式碼。
影響系統	Apache Struts 2.3.20 至 Apache Struts 2.3.28(2.3.20.2、2.3.24.2 除外。
建議解決方法	1. 建議使用者應儘速將 Apache Struts 2 更新至 2.3.20.2、2.3.24.2 或 2.3.28.1 以上之版本。 2. 相關網站： https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3081 http://www.securitytracker.com/id/1035665 http://struts.apache.org/download.cgi#struts-ga

＊OpenSSL patches two high-severity flaws

說明	高嚴重性漏洞的代號CVE-2016-2107為ASN.1解碼器在解析字串時存在弱點，可能導致瀏覽器崩潰。另一個高嚴重性漏洞CVE-2016-2108 為兩個低風險漏洞所構成，並可能導致 OpenSSL 崩潰。
影響	遠端攻擊者可利用此弱點，執行任意程式碼。
影響系統	OpenSSL 1.0.1t 與 OpenSSL 1.0.2h。
建議解決方法	1. 建議使用者應儘快升級至最新版本。 2. 相關網站： https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2107 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2108 https://www.openssl.org/news/vulnerabilities.html https://www.openssl.org/source/

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)
  - MD5：437994adc7afa54220c02a78032a9978
  - SHA-1：3c1f2766ebfc58a90004535f253e9b1af5175c5d
- 惡意程式檔案大小： 1,406,419 bytes
- 各防毒軟體定義名稱：
  - Avira：EXP/CVE-2012-1856.46556
  - BitDefender：Exploit.RTF-ObfsStrm.Gen
  - Fortinet：MSOffice/CVE_2015_1641.A!exploit
  - TrendMicro：TSPY_FAREIT.BYX

(2)惡意程式行為分析

- 利用 Microsoft Office 的漏洞進行攻擊：此惡意程式利用 CVE-2015-1641 這個漏洞，針對 Microsoft Office 的 Word 發動攻擊，受影響的版本包含 Microsoft Word 2007, Microsoft Office 20140 以及 Microsoft Word 2010。微軟已就以漏洞，發布 MS15-033 的重大安全性更新。
- 存取主機系統資訊：此惡意程式在感染主機後，會試圖存取主機的系統資訊，例如讀取 MachineGuid、DigitalProductid 與 SystemBiosDate。
- 修改啟動清單：該惡意程式在感染主機後，會修改受害電腦的系統啟動清單，藉由偽裝為系統服務，讓受害主機每次都會重新啟動該程式。
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\OSession
- 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：henry.myftp.biz
     ✓ IP：104.244.153.127 國家：美國

(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