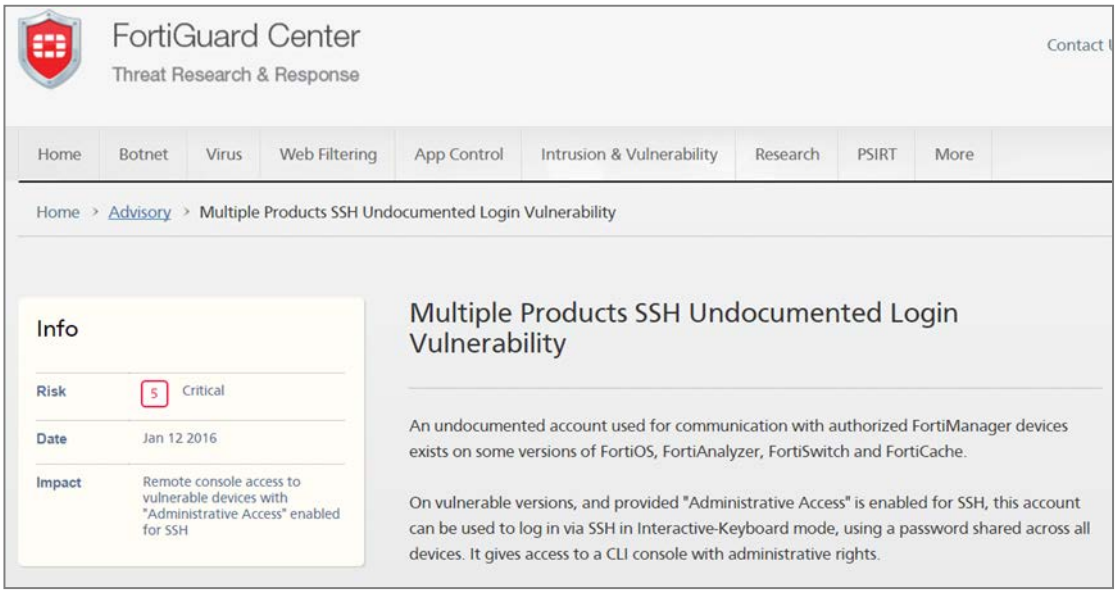
一、弱點知識庫

＊Cisco UCS 管理軟體和 Firepower 9000 系列設備存在安全性弱點

說明	UCS 管理軟體（UCS Manager）和 Firepower 9000 系列設備存在安全性弱點。在 CGI 腳本程式中，Shell Command 未受保護的呼叫，遠端攻擊者可利用此弱點發送特製的 HTTP 請求至 UCS Manager 和 Firepower 9000 系列設備，並執行任意程式。
影響	遠端攻擊者可利用此弱點，執行任意程式。
影響系統	-UCS Manager 受影響的版本包含 2.2（4b）、2.2（5a）和 3.0（2e），以及 2.2.x 之前的版本。 -Firepower 9000 系列設備受影響的版本 1.1.2 之前的版本。
建議解決方法	1. 建議使用者應儘速更新至最新版本 2. 相關網站： http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160120-ucsm https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6435

＊Multiple Products SSH Undocumented Login Vulnerability

說明	Fortinet 多項產品中存在驗證問題，這隻名為 FortiGuard SSH (Secure Shell)後門程式，是源自一項管理功能的結果，它允許未記錄(undocumented)的帳號及寫死的密碼。
影響	遠端攻擊者可取得管理員權限。
影響系統	-FortiAnalyzer: 5.0.5、5.0.11 與 5.2.0 至 5.2.4 版本 -FortiSwitch: 3.3.0 至 3.3.2 版本 -FortiCache: 3.0.0 至 3.0.7 版本 -FortiOS 4.1.0 至 4.1.10 版本 -FortiOS 4.2.0 至 4.2.15 版本 -FortiOS 4.3.0 至 4.3.16 版本 -FortiOS 5.0.0 至 5.0.7 版本
建議解決方法	1. 建議使用者應儘速更新至最新版本： -FortiAnalyzer：升級到 5.0.12 或 5.2.5 版本以上 -FortiSwitch：升級到 3.3.3 版本 -FortiCache：升級到 3.0.8 版本 -FortiOS：升級到 4.1.11 版本以上 2. 相關網站： http://www.fortiguard.com/advisory/multiple-products-ssh-undocumented-login-vulnerability



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)
  - MD5：0a5d10bef6c5f91b6c1bf1c0ae762b46
  - SHA-1：ffeda15ad72bebbff5ab9d2c9600a03002266192
- 惡意程式檔案大小： 211,968 bytes
- 各防毒軟體定義名稱：
  - NOD32：Win32/Virut.AV
  - Avira：W32/Virut.AX
  - Symantec：W32.IRCBot
  - McAfee：W32/Virut.gen.a

(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:\DOCUME~1\User\LOCALS~1\Temp\jpccx.bat
  - C:\DOCUME~1\User\LOCALS~1\Temp\0a5d10bef6c5f91b6c1bf1c0ae762b46.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：japan.youngpeyatech.info
    - ✓ IP：無　　國家：無
  - B. 網域名稱：preek.oihduhdd.net
    - ✓ IP：無　國家：無

(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