一、弱點知識庫

＊NTP 安全漏洞恐導致 DDoS 分散式阻斷服務攻擊

說明	網路時區基金會(Network Time Foundation)的 NTP project 已發布多個 NTPD 漏洞更新。其中有一個屬於高度嚴重漏洞是 CVE-2016-4957，相關漏洞可造成 NTPD 當掉而招致分散式阻斷服務攻擊。
影響	該漏洞可能造成分散式阻斷服務攻擊。
影響系統	NTP 4.2.8p8 之前版本。
建議解決方法	1. 建議使用者應儘速將目前使用版本更新至最新之版本。 2. 相關網站： http://nwtime.org/ntf-releases-ntp-4-2-8p8-security-patch/ https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4957

圖片來源：https://threatpost.com/ntp-patches-flaws-that-enable-ddos/118470/

＊Symantec Decomposer Engine Multiple Parsing Vulnerabilities

說明	賽門鐵克旗下產品存在多項高風險漏洞，可能導致遠端攻擊者取得使用者電腦控制權限。這些漏洞，不需要任何使用者互動就能產生危害，而且可以最高權限執行。其中名為 CVE-2016-2208 的漏洞存在賽門鐵克用於過濾執行檔封裝程式(packer)的軟體中，在 Linux、Mac 或其他 Unix 平台上，會引發堆積緩衝區溢位(heap overflow)攻擊，而在 Windows 平台則可能導致核心記憶體毀損。
影響	遠端攻擊者可能藉此漏洞取得使用者電腦控制權限。
影響系統	- Advanced Threat Protection (ATP)　2.0.3(含)之前版本。 - Symantec Data Center Security:Server (SDCS:S) 6.6MP1 之前版本。 - Symantec Endpoint Protection (SEP) 、(SEP for Mac) 、(SEP for Linux)12.1.6 MP4 (含)之前版本。 -Symantec Protection Engine (SPE) 7.8.0 之前版本。 -Symantec Protection for SharePoint Servers (SPSS) 6.0.6(含)之前版本。 -Symantec Mail Security for Microsoft Exchange (SMSMSE) 7.5.4(含)之前版本。 -Symantec Mail Security for Domino (SMSDOM) 8.1.3(含)之前版本。 -CSAPI 10.0.4 (含)之前版本。 -Symantec Message Gateway (SMG) SMG 10.6.1-3 (含)之前版本。 -Norton Product Family All Prior to NGC 22.7 。 -Norton Security for Mac 13.0.2 之前版本。 - Norton Power Eraser (NPE) 5.1 之前版本。 - Norton Bootable Removal Tool (NBRT) 2016.1 之前版本。
建議解決方法	1. 建議使用者應儘速將目前使用版本更新至最新之版本。 2. 相關網站： https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160628_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

- 單一識別碼(Hash 值)
  - MD5：d7a4cfdfae7a885398e60554b1ae17a4
  - SHA-1：bc6bbadc3e22a3ad74e7ade8ac5ddfc7ad42f587
- 惡意程式檔案大小： 934,352 bytes
- 各防毒軟體定義名稱：
  - Avast：Win32:Malware-gen
  - BitDefender：Trojan.GenericKD.3297469
  - Fortinet：MSIL/Injector.PLI!tr
  - McAfee：Artemis!D7A4CFDFAE7A

(2)惡意程式行為分析

- 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_USERS\\S-1-5-21-1547161642-507921405-839522115-1004\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon
- 干擾砂箱分析作業，此惡意程式會透過休眠(Sleep)的指令，在感染受害主機後會靜止 1,566,904 秒(超過 18 天)。
- 對外發起 HTTP 連線請求，連線之外部主機資訊如下：
  - cacerts.digicert.com
    IP：72.21.91.29　國家：美國
  - www.download.windowsupdate.com
    IP：65.118.123.162　國家：美國
  - DonkeyPunched.csgoblock.com
    IP：82.196.15.50　國家：荷蘭

(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
- Google Chrome Cleanup Tool, 官方網站：
  https://www.google.com/chrome/cleanup-tool/