一、弱點知識庫

＊glibc getaddrinfo stack-based buffer overflow

說明	在 Glibc 的 DNS 客戶端解析器中使用 getaddrinfo() 函式功能時，遠端攻擊者只要在合法的 DNS 請求時，以過大的 DNS 檔案回應，便會形成堆積緩衝區溢位漏洞。
影響	遠端攻擊者可利用此弱點，執行中間人攻擊。
影響系統	Glibc 2.9 以後的所有版本。
建議解決方法	1. 建議使用者應儘速修補。修補程式： https://sourceware.org/ml/libc-alpha/2016-02/msg00416.html 2. 相關網站： https://googleonlinesecurity.blogspot.tw/2016/02/cve-2015-7547-glibc-getaddrinfo-stack.html?m=1

＊Squid.HTTP.Host.Header.Port.Handling.DoS

說明	Squid Cache（簡稱為 Squid）是 HTTP 代理伺服器軟體。Squid 用途廣泛，可以作為快取伺服器，可以過濾流量幫助網路安全，也可以作為代理伺服器鏈中的一環，向上級代理轉發資料或直接連線網際網路。遠端攻擊者利用 Squid 中的 client_side_request.cc 檔案在處理 HTTP 請求時存在弱點，透過發送惡意變造含有不正確標頭 Host 埠號碼值的 HTTP 請求來造成錯誤，進而導致服務終止達成阻斷服務攻擊(denial of service)。
影響	攻擊者可能利用 Squid 中的 client_side_request.cc 檔案在處理 HTTP 請求時存有的弱點發動 DoS 攻擊。
影響系統	-Squid 3.2 版到 3.2.13 的版本。 -Squid 3.3 版到 3.3.8 的版本。
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.檢視及執行各系統之安全修補，並將 Squid 更新至最新版本。官方參考網站： http://www.squid-cache.org/Advisories/SQUID-2013_3.txt

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：c1d267be41c8dbcf982a3fe01ed857c6
  - SHA-1：a8593802ffb1c1e4db38abd9c8b65eb28cc5f05c
- 惡意程式檔案大小： 1,522,176 bytes
- 各防毒軟體定義名稱：
  - Avast：MSIL:GenMalicious-APD [Trj]
  - BitDefender：Gen:Variant.Kazy.469353
  - F-Secure：Gen:Variant.Kazy.469353
  - Kaspersky：HEUR:Trojan.Win32.Generic

(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:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\machine.config
  - C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\config\security.config.cch
  - C:\Documents and Settings\User\Local Settings\Temp\server.exe (惡意程式，VirusTotal 偵測結果為 39/55)
- 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
    - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- 程式偽裝：該惡意程式使用 MicroSoft Windows Live Messenger 的檔案資訊作進行偽裝。
- 修改防火牆政策：該惡意程式透過修改機碼的方式，調整受害主機的防火牆規則，變更其防火牆針對網際網路以及內部網路之安全設定。
  - HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Sec

urity\Policy\Extensions\NamedPermissionSets
- HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\Internet
- HKEY_LOCAL_MACHINE\Software\Microsoft\.NETFramework\Security\Policy\Extensions\NamedPermissionSets\LocalIntranet

➢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:

網域名稱：simon93.ddns.net(動態 dns 網域名稱)

IP：82.205.78.132　　國家：巴勒斯坦

(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