教育部 98 年度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
惡意程式分析報告
efed811e135fc1ff45d073667bda6e73

國家高速網路與計算中心

2011 年 11 月 09 日

目錄

一、前言

本文主要針對教育部 98 年度教育學術資訊安全監控中心(A-SOC)暨殭屍電腦(Botnet)防禦機制建置計畫中藉由 Honeynet 誘捕系統所蒐集到之惡意程式進行分析說明，其報告內所分析之惡意程式主要以誘捕系統每月所偵測到之攻擊比率最高者為分析對象，如有重複則以次高或次次高者為主。

二、惡意程式分析

本報告針對 2011 年十月份由 Honeynet 誘捕系統所偵測到之惡意程式攻擊數較高者為分析對象，其惡意程式之資訊與相關行為如下述分析:

- 惡意程式 MD5: efed811e135fc1ff45d073667bda6e73
- 惡意程式 SHA-1: a5a565c28f26cbbdfbb844c321d4f644d731dcbf
- 惡意程式大小：125,440　bytes
- 防毒軟體定義名稱:
  - Virus.Win32.Sality.ag (Kaspersky)
  - W32/Sality.gen.z (McAfee)
  - Worm:Win32/Korgo.S (Microsoft)
  - PE_SALITY.RL (TrendMicro)
  - W32.Sality.AE (Symantec)
- 惡意程式行為分析
  - 修改系統機碼，禁止直行 Regedit 指令。
  - 此惡意程式執行後將會自行複製到”%System%目錄下，如 Windows XP 下則會在 C:\WINDOWS\system32\目錄下，而誤惡意程式名稱通常為隨機字元.exe，如 siocfpib.exe
- 註冊碼修改
  - 惡意程式執行後，將會針對註冊碼進行一連串的修改，以確保該惡意程式於開機時即自動執行。
    - 建立" HKEY_LOCAL_MACHINE \Software\Microsoft\Wireless"
    - 於"HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Wireless\”新增 key 值 Client=1
    - 於" HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Wireless\”新增 key 值 ID= 隨機字串"
      - Ex: ID= fgxhjbwbjdkhclom
    - 於 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 新增 key 值 System Update "%System%\隨機字元.exe"

◆ Ex: System Update=C:\WINDOWS\system32\siocfpib.exe

➢ 刪除註冊表 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wireless\下的 Client 值。

◆ 以上註冊碼之行為，於本分析案例中將使系統開機後自動執行 siocfpib.exe 之惡意程式

➢CC Server:213.155.0.224:80

➢DNS Lookups: moscow-advokat.ru、acemoglusucuklari.com.tr

➢網路行為分析

◆ 當惡意程式執行後，將會針對 moscow-advokat.ru、acemoglusucuklari.com.tr 進行 Domain Name 解析

➢使用者自我檢查：

使用者可從其上述註冊碼中自我檢查判斷是否感染惡意程式。

➢ 其他參考資料:

◆ http://www.threatexpert.com/report.aspx?md5=efed811e135fc1ff45d073667bda6e73