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
87136C48890347463036 9E232704FA4D

國家高速網路與計算中心

2011 年 12 月 13 日

目　　錄

一、前言

本文主要針對教育部 98 年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 11 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: 87136C488903474630369E232704FA4D
- 惡意程式 SHA-1: C2A8998F34FB6FE505635E0AC352CE2838A3ACA6
- 惡意程式大小：164,746 bytes
- 防毒軟體定義名稱:
  - Worm.Conficker (PCTools)
  - Worm.Conficker(PCTools)
  - Trojan-Downloader.Win32.Kido.bu (Kaspersky Lab)
  - W32/Conficker.worm(McAfee)
  - Mal/Conficker-A (Sophos)
  - Worm:Win32/Conficker.C (Microsoft)
  - Trojan-Downloader.Win32.Kido (Ikarus)
  - Win32/Conficker.worm.164746 (AhnLab)
- 惡意程式行為分析
  - 修改系統機碼，禁止直行 Regedit 指令。
  - 此惡意程式將會利用網路進行弱點攻擊，具備 Conficker/Downadup/Kido 的蠕蟲特性，並且運用微軟 Windows Server 中的 RPC 服務，利用 RPC 遠程控制代碼漏洞進行傳播，並會嘗試修改受害主機防火牆之設定以及停用安全更新的服務，例如：Windows Update、Norton Update、Kaspersky Update 等，感染後此程式會自動將 IP 位址洩露到中繼站，另會運用隨身碟的自動播放機制，新增 Autorun.inf 檔案到隨身碟等外接 USB 儲存裝置上，以做為下次感染的管道。
- 對於系統的影響，將會嘗試開啟以下幾個磁碟路徑：
  - ADMIN$、C$、E$、IPC$
  - 並嘗試使用以下字串進行字典攻擊：
    - 00000、000000、00000000、111111、11111111、123123、12345、123456、1234567、12345678、123456789、1234qwer、123abc、123asd、123qwe、

54321、654321、88888888、abc123、academia、admin、admin$、admin123、administrator、admins、america、anchor、anything、april、arrow、artist、asdfgh、basic、changeme、cluster、codeword、coffee、compaq、cookie、country、dirty、drive、email、england、english、forever、france、freedom、french、ghost、ihavenopass、india、input、japan、julie、killer、letmein、logout、macintosh、modem、monday、mouse、mypass、mypc123、network、nobody、pass123、password1、password123、phone、phrase、private、pw123、right、saturday、script、simple、student、superuser、target、temp123、test123、thailand、user1、video、virus、xxxxx、xxxxxx、xxxxxxxx、xxxxxxxxx

➢其他參考資料:

- http://www.threatexpert.com/report.aspx?md5=87136C488903474630369E232704FA4D