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
f3d217396bd1b42d189e8b9ddfbf4f99

國家高速網路與計算中心

2011 年 5 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 年四月份由 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: f3d217396bd1b42d189e8b9ddfbf4f99
- 惡意程式 SHA-1: 094d7d4cbf60ffd238f7a8e93ef313d9d3a39088
- 惡意程式大小：86,528 bytes
- 防毒軟體定義名稱:
  - Worm/Korgo.A (AVG)
  - W32/Sality.gen.z (McAfee)
  - Worm:Win32/Korgo.V (Microsoft)
  - PE_SALITY.RL (TrendMicro)
  - W32.Sality.AE (Symantec)
- 惡意程式行為分析
  - 惡意程式執行後會產生 autorun.inf 隱藏檔案於系統碟目錄下(C:\)
  - regedit 指令將會被停用。
  - 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，而惡意程式名稱通常為隨機字元.exe，如 xrbtqau.exe
  - 修改系統安全設定
  - 賽門鐵克防毒軟體於該程式執行後，將會偵測到 OS Attack:MS RPC LSASS OS Oversized Request TCP 攻擊流量攻擊，該攻擊主要針對 CVE-2003-0533(MS04-011)之系統漏洞。
- 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= zpesyqsmyfpcaxs

➢ 於 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 新增 key 值 Cryptographic Service= "%System%\隨機字元.exe"

◆ Ex: Cryptographic Service=C:\WINDOWS\system32\xrbtqau.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 xrbtqau.exe 之惡意程式

➢CC Server:

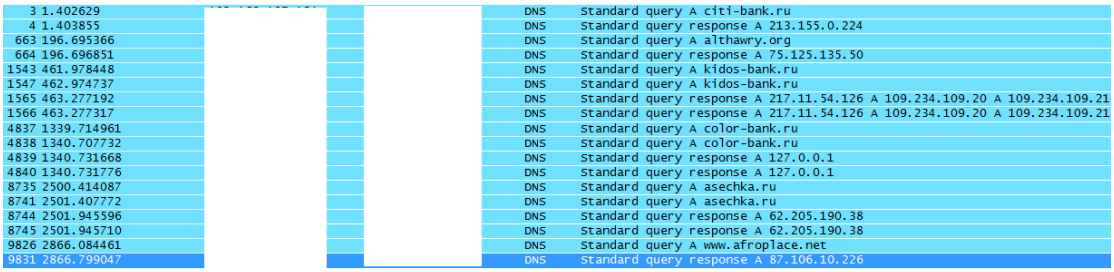
◆ 213.155.0.224:80、75.125.135.50:80、217.11.54.126:80、109.234.109.20:80、109.234.109.21:80、109.234.109.55:80、217.11.52.234:80、193.46.215.55:80、62.205.190.38:80、213.248.61.180:80、213.248.62.3:80、87.106.10.226:80

➢DNS Lookups

◆ citi-bank.ru 、 althawry.org 、 kidos-bank.ru 、 color-bank.ru 、 asechka.ru 、 www.afroplace.net

➢網路行為分析

◆ 當惡意程式執行後，會友針對上述之 DNS 進行查詢解析，其過程如下:

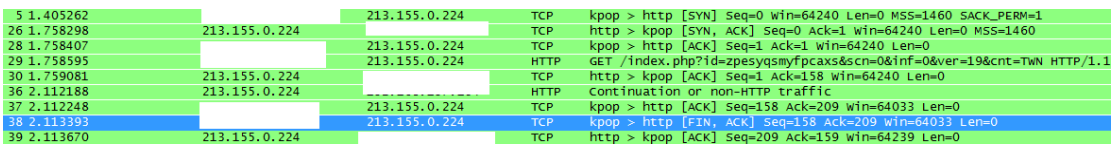


3	1.402629			DNS	Standard query A citi-bank.ru
4	1.403855			DNS	Standard query response A 213.155.0.224
663	196.695366			DNS	Standard query A althawry.org
664	196.696851			DNS	Standard query response A 75.125.135.50
1543	461.978448			DNS	Standard query A kidos-bank.ru
1547	462.974737			DNS	Standard query A kidos-bank.ru
1565	463.277192			DNS	Standard query response A 217.11.54.126 A 109.234.109.20 A 109.234.109.21
1566	463.277317			DNS	Standard query response A 217.11.54.126 A 109.234.109.20 A 109.234.109.21
4837	1339.714961			DNS	Standard query A color-bank.ru
4838	1340.707732			DNS	Standard query A color-bank.ru
4839	1340.731668			DNS	Standard query response A 127.0.0.1
4840	1340.731776			DNS	Standard query response A 127.0.0.1
8735	2500.414087			DNS	Standard query A asechka.ru
8741	2501.407772			DNS	Standard query A asechka.ru
8744	2501.945596			DNS	Standard query response A 62.205.190.38
8745	2501.945710			DNS	Standard query response A 62.205.190.38
9826	2866.084461			DNS	Standard query A www.afroplace.net
9831	2866.799047			DNS	Standard query response A 87.106.10.226

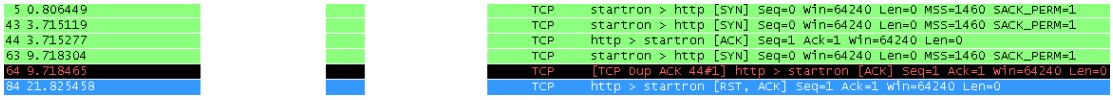
◆ 並針對 213.155.0.224 之位址，發現惡意程式有進一步的網路行為，其將會透過該網址發出 HTTP GET 請求(詳見下圖)，其請求如下

➢ GET /index.php?id=zpesyqsmyfpcaxs&scn=0&inf=0&ver=19&cnt=TWN

該請求疑似透過 index.php 來告訴遠端主機已遭感染之主機之資訊，如 ID 為 zpesyqsmyfpcaxs (對應到註冊碼之 ID Key 值)，而其所在國家為 TWN。



5	1.405262		213.155.0.224	TCP	kpop > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
26	1.758298	213.155.0.224		TCP	http > kpop [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
28	1.758407		213.155.0.224	TCP	kpop > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
29	1.758595		213.155.0.224	HTTP	GET /index.php?id=zpesyqsmyfpcaxs&scn=0&inf=0&ver=19&cnt=TWN HTTP/1.1
30	1.759081	213.155.0.224		TCP	http > kpop [ACK] Seq=1 Ack=158 Win=64240 Len=0
36	2.112188	213.155.0.224		HTTP	Continuation or non-HTTP traffic
37	2.112248		213.155.0.224	TCP	kpop > http [ACK] Seq=158 Ack=209 Win=64033 Len=0
38	2.113393		213.155.0.224	TCP	kpop > http [FIN, ACK] Seq=158 Ack=209 Win=64033 Len=0
39	2.113670	213.155.0.224		TCP	http > kpop [ACK] Seq=209 Ack=159 Win=64239 Len=0



➢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。

如未預期的 regedit 指令功能被停用也極可能已感染病毒。

➢預防措施:

此惡意程式主要是運用 CVE-2003-0533-"MS04-011 Lsasrv.dll RPC buffer overflow remote exploit”針對 Windows XP 與 Windows 2000 的 LSASS(本地安全性授權子系統服務)弱點進行攻擊，其所使用之通訊埠為 445，一但攻擊成功便植入 ShellCode，攻擊者便可以經由指定的通訊埠對被攻擊的電腦下指令，完全控制受害的電腦。關於 MS04-011 之弱點與更新資訊可從其微軟網站查看與下載更新檔:

◆ http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0533

◆ http://www.microsoft.com/technet/security/bulletin/ms04-011.mspx

➢移除方法

由於該惡意程式分析環境為在虛擬機上安裝 Windows XP2 作業系統，再測試移除的方法中發現微軟線上掃描似乎可針對此惡意程式進行移除，因此建議如發現遭受此惡意程式感染時，可嘗試透過微軟提供的免費掃描工具來移除該感染之惡意程式，其微軟提供的免費掃描工具網址如下:

◆ http://www.microsoft.com/security/scanner/zh-tw/default.aspx