財團法人國家實驗研究院
國家高速網路與計算中心
National Center for High-Performance Computing

惡意程式誘捕

Nepenthes、Dionaea

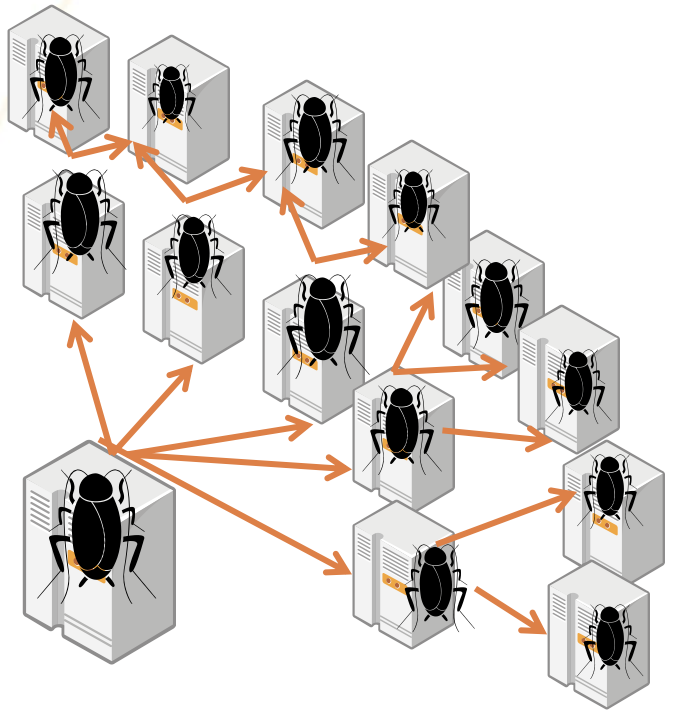
蔡一郎

大綱

- Malware Introduction
- Low interaction honeypots

What is Malware ?

- Malware = **Malicious + Software**
  - Software programs that serve *malicious purposes are usually called malware.*
  - 惡意程式是指未經使用者許可情況下，在使用者的電腦主機上安裝運行，侵犯用戶隱私與合法權益之程式，Virus, Worm, Trojan, backdoor, Spyware, …



Malware Introduction (Cont.)

- 散播方法:
  - 惡意網站，惡意連結
  - 即時通訊程式
  - 網路共用
  - 電子郵件附檔
- 特性:
  - 快速變種與演化
  - 強制安裝，難以移除
  - 綁架瀏覽器，瀏覽特定網站
  - 收集並洩漏使用者隱私資訊
  - 遭受遠端控制，執行惡意行為

Malware Introduction (Cont.)

- 惡意程式來源：
  - 各式各樣網站都可能被駭客植入惡意程式，成為惡意程式下載點
  - 郵件附檔，惡意程式執行檔、惡意文件(Word、PDF、Excel、Zip)
  - 沒有安裝更新程式(Patch)作業系統、沒有安裝防毒軟體，容易遭受惡意程式感染。
  - 瀏覽惡意網頁，將使用者電腦導向到惡意程式下載點，下載惡意程式
  - USB
- 惡意程式流行趨勢：
  - 帳號竊取程式
  - 監控與遠端遙控程式
  - 具反監控與反移除功能(停止防毒軟體運行與更新）
  - 文件型病毒大量發展與散佈

駭客為何要發展惡意程式？

工欲善其事，必先利其器

目的1: 竊取個資

入侵使用者電腦，竊取個人帳號、密碼、控制Webcam，電子郵件社交攻擊，釣魚網站。

目的2: 系統控制

控制利用使用者系統資源，遠端攻擊他人，強迫使用者瀏覽特定網站，亂發廣告信。

目的3: 獲取利益

販賣個人資料、銀行帳戶號碼給詐騙集團。販賣系統控制權，販賣惡意程式

工具1： 惡意程式

創造不同功能的惡意程式，如：帳號竊取程式，病毒、遙控木馬，PDF病毒。

工具2： 散佈管道

創造暢通的中毒管道，擴大感染範圍，垃圾郵件，惡意網站，社交網站、通訊軟體。

工具3： 攻擊時效性

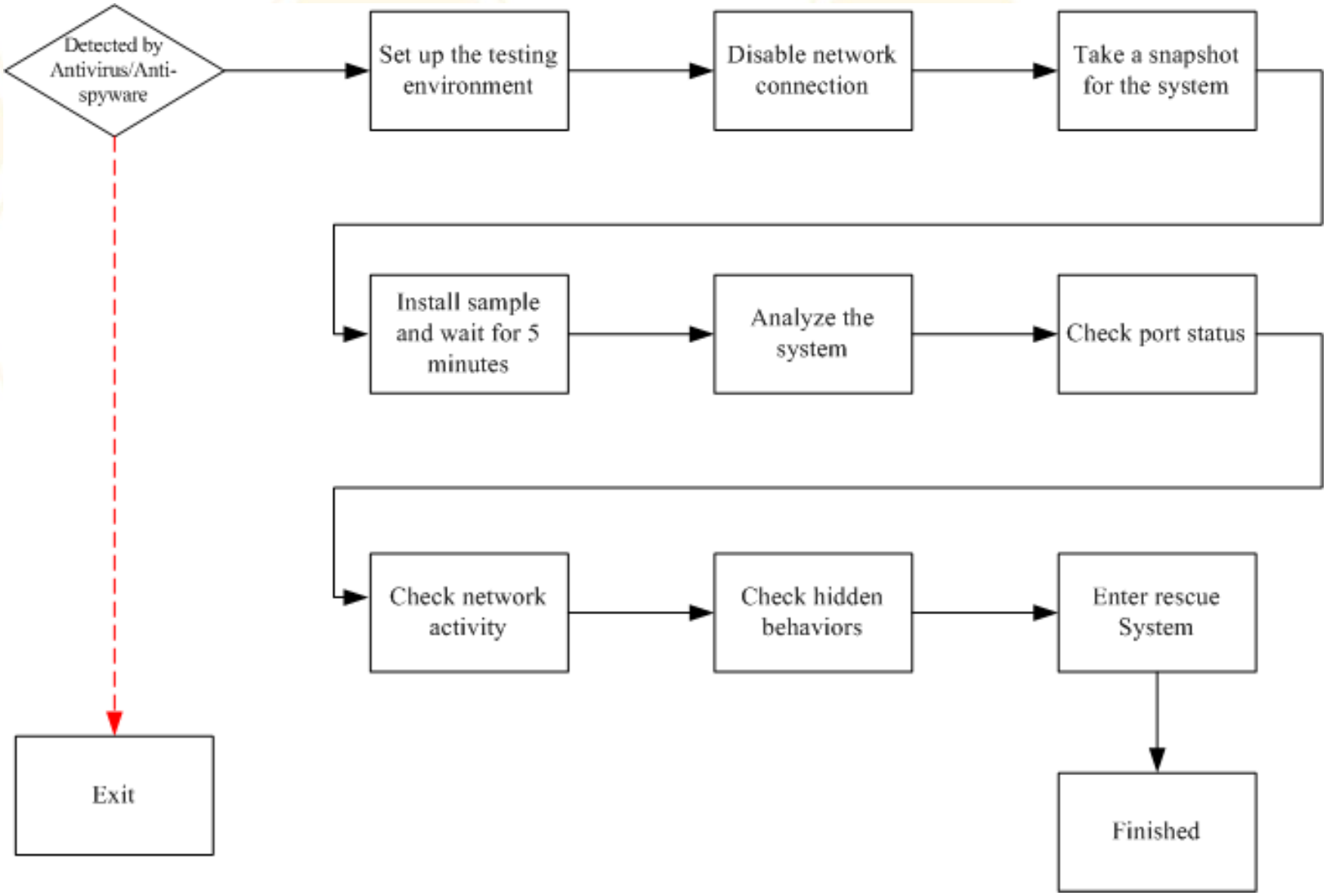
地下駭客市場，販賣簡易好用的惡意程式產生器，與最新惡意程式，減少駭客準備時間，增加工及時效性。團結力量大，善用團隊分工合作。

Malware Introduction (Cont.)

- 為何要收集惡意程式?

- Learn more about *attack patterns, attack trends, attack rates, spread method, malicious network activities, based on live and authentic data*

惡意程式的分析流程


Detected by Antivirus/Anti-spyware
Set up the testing environment
Disable network connection
Take a snapshot for the system
Install sample and wait for 5 minutes
Analyze the system
Check port status
Check network activity
Check hidden behaviors
Enter rescue System
Finished
Exit

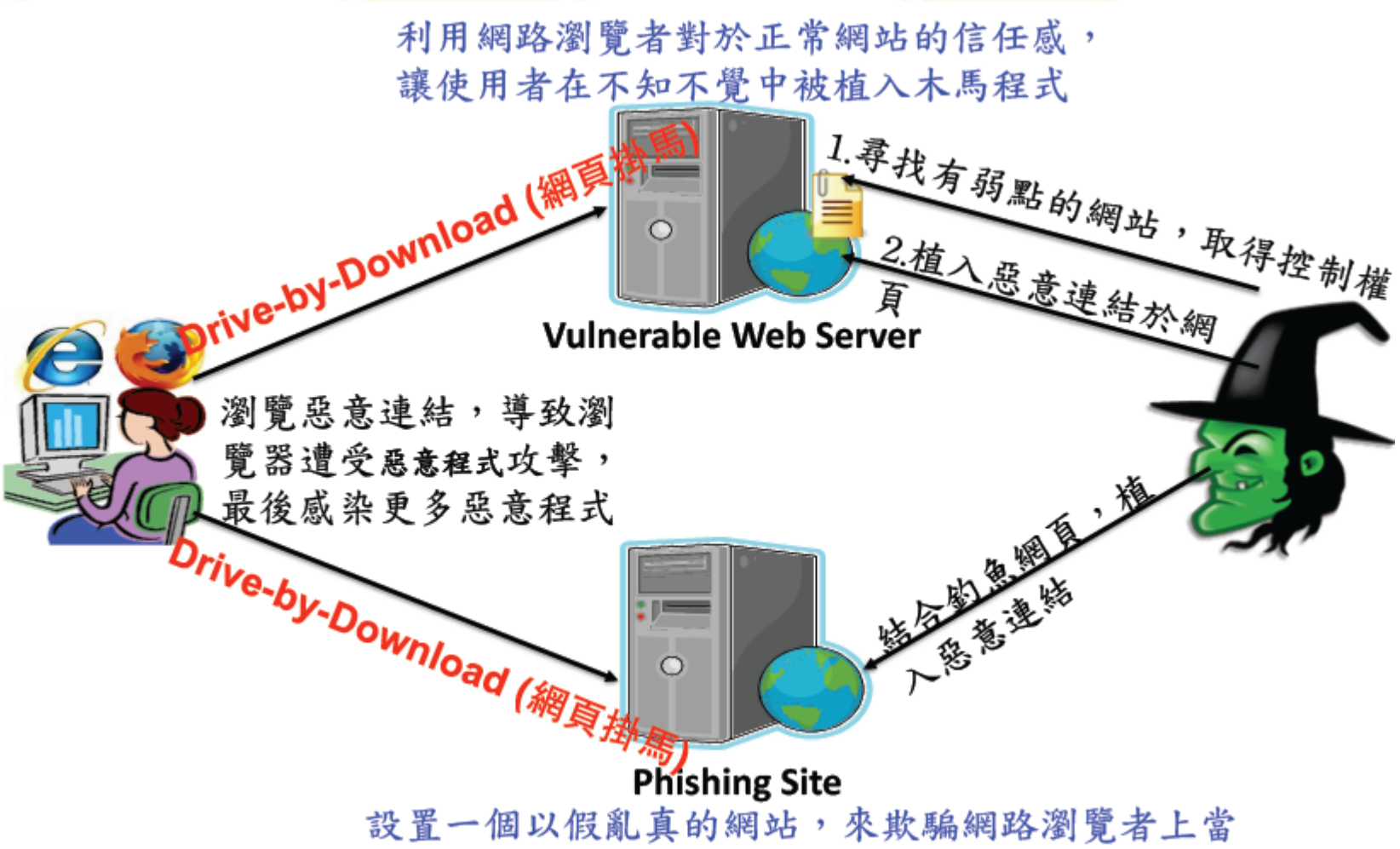
相關工具

- Process Monitor - Process explorer
- File Monitor - Filemon
- Registry Monitor - Regmon
- Port Monitor
  - Netstat
  - TCPView
  - TDIMon
  - Fport
- Network Monitor – Ethereal
- All-In-One System Analysis Tool – InstallRite, HijackThis, SREng
- Rootkit Detection Tools
  - IceSword
  - RootkitRevealer
  - BlackLight
- File Integrity Check – MD5 or Tripwire
- Windows Live CD – WinPE or BartPE

惡意程式散佈管道－惡意網頁攻擊模式分析

- 駭客攻陷有弱點網站，植入惡意連結或惡意程式於網頁中，或建造釣魚網站，誘騙使用者瀏覽惡意網頁。
- 當使用者瀏覽惡意網頁時，惡意程式將攻擊使用者系統，感染使用者電腦系統弱點或是瀏覽器，竊取受害者個人資訊，控制系統資源。
- 任何網站皆有可能成為惡意網站，網站管理者需做好安全防護措施。盡量不要瀏覽中國大陸網站，下載檔案。
- 防毒軟體無法完全有效偵測惡意網站

惡意程式散佈管道 – 惡意網頁攻擊模式分析 (Cont.)

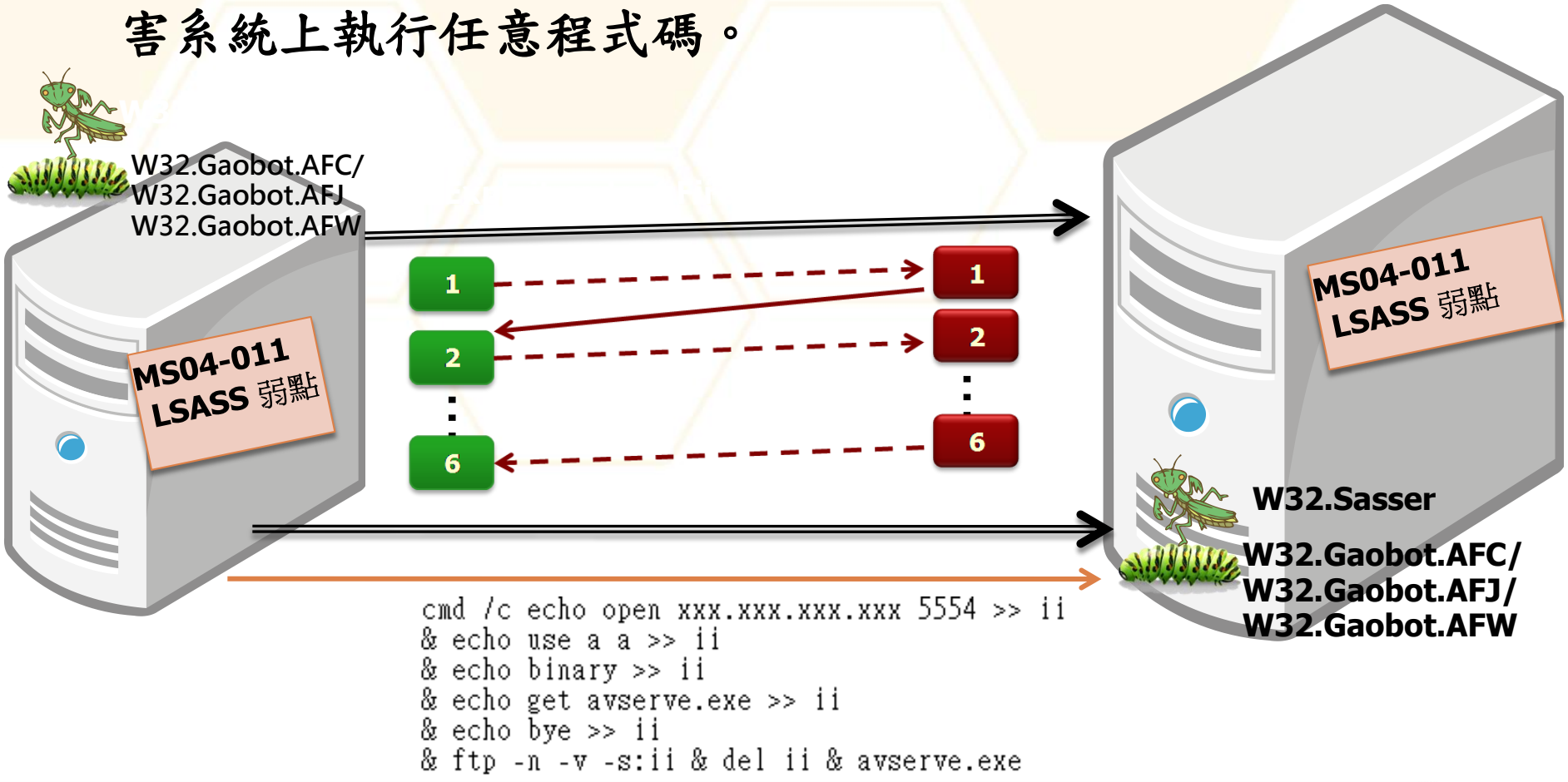


惡意程式散佈管道－社交工程手法

- 社交工程為駭客利用非技術性手段，降低使用者防禦心，進而獲得隱私性資料並取得控制權。社交工程通常運用於特定目標對象，與釣魚網站相結合。
- 三大手段：
  - 電子郵件社交工程：駭客偽冒寄件者發送惡意郵件，郵件內容以吸引人內容或是特惠，或運用人際關係，誘騙受害者瀏覽並點閱電子郵件中之連結或是附加檔案。導致受害者連結到釣魚網站或是惡意網站，遭受惡意程式感染。
  - 通訊軟體MSN、Skype社交工程：駭客偽冒受害者之好友，發送惡意連結或是傳送惡意程式，一旦受害者點閱連結或執行惡意程式，駭客將可竊聽受害者通訊內容，取得個人隱私權資料。
  - 網路釣魚(Phishing)：要求或發動詐騙以取得個人機密資訊的欺詐性網站。駭客利用電子郵件發送釣魚網站連結，釣魚網站抄襲熱門網站或公司的外觀。詐騙網站會要求你提供個人資訊，例如信用卡號碼、身分證號碼或帳戶密碼等。

惡意程式運作實例– LSASS Vulnerability

- MS04-011(CVE 2003-0533)：對LSASRV.DLL 進行緩衝區溢位攻擊成功後，可取得系統控制權，遠端攻擊者可在受害系統上執行任意程式碼。



惡意程式運作實例– LSASS Vulnerability

- MD5:
  - 7d99b0e9108065ad5700a899a1fe3441
- SHA-1:
  - 5AB1A63CFCA5BE0DAC591194583F6405C16905DD
- 大小：9,353 bytes
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
  - Cryptographic Service = “%System%\隨機字元.exe”
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Wireless
  - ID
  - Client

Most Aggressively Spreading Malware Binaries

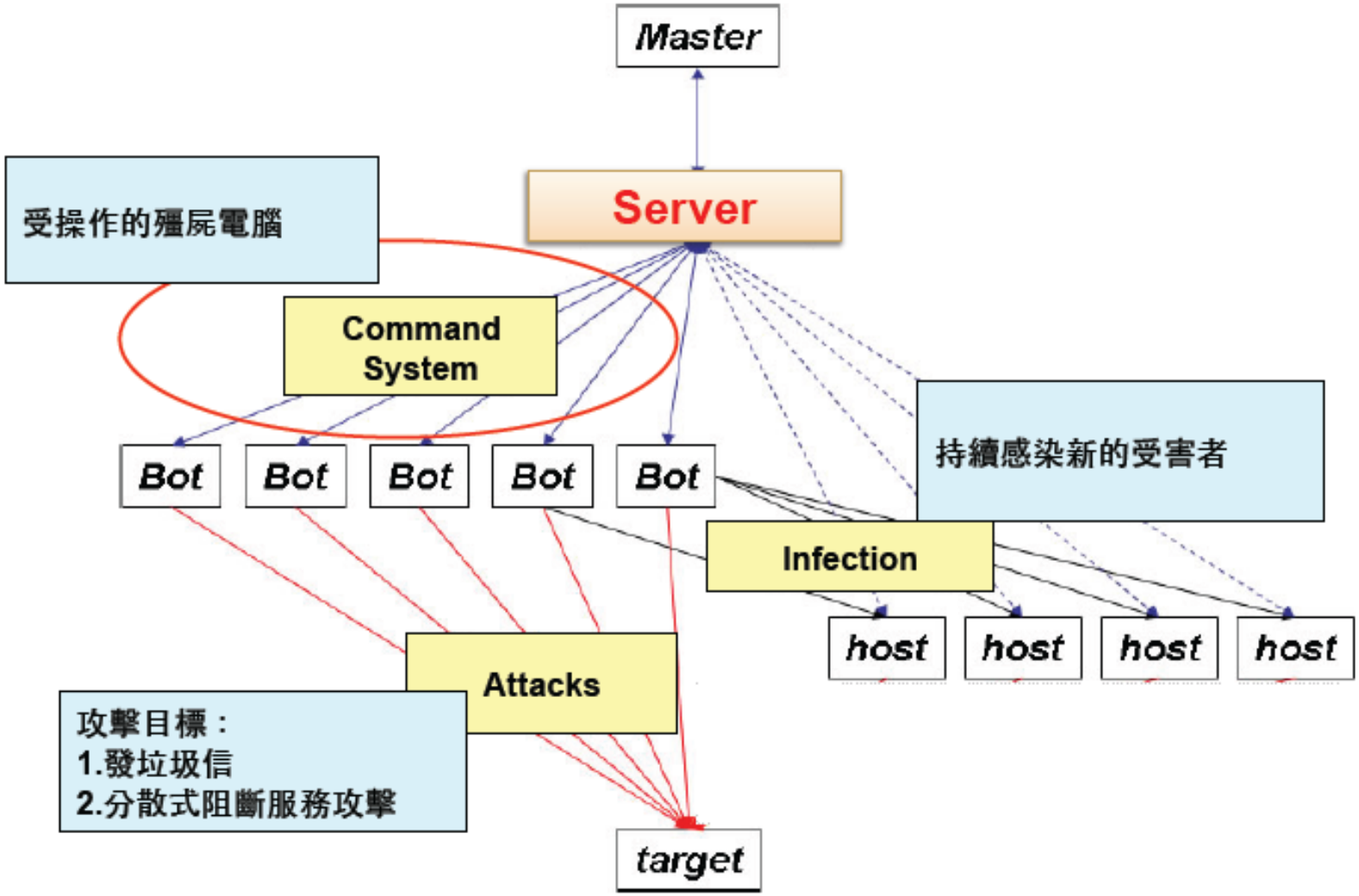
Mon Sep 13 08:53:29 2010

rank	hits	first	last	AV rate	Binary MD5
55		08/27	09/12	0 of 32	d41d8cd98f00b204e9800998ecf8427e
6		08/27	09/11	2 0 of 32	ca832de942ad18471ca9a38ffe3cf7a9
5		08/17	08/26	33 0 of 32	53bfe15e9143d86b276d73fdcaf66265
4		08/27	09/10	2 0 of 32	9ba1f1416a20fd97cdd2fcd9b45c08a9
3		08/17	08/26	26 of 32	7d99b0e9108065ad5700a899a1fe3441
3		08/27	09/10	0 0 of 32	c9b4b7f0b994b5f2322b03140a5170da
2		08/27	09/10	0 0 of 32	14335fc76500b701cb44f20d56e3eeb1
1		08/28	09/08	0 0 of 32	20c94c7ab1bc0632ac467edf3642ac85
1		08/28	09/09	0 0 of 32	c72eeb095200f2676fea0c9aef80791e
1		08/27	09/07	0 0 of 32	13923caf716e04c4c11a465233094b30

Malware THREAT CENTER

- http://www.mtc.sri.com/
- http://www.cyber-ta.org/releases/malware-analysis/public/SOURCES/

From Malware to Botnet (Cont.)



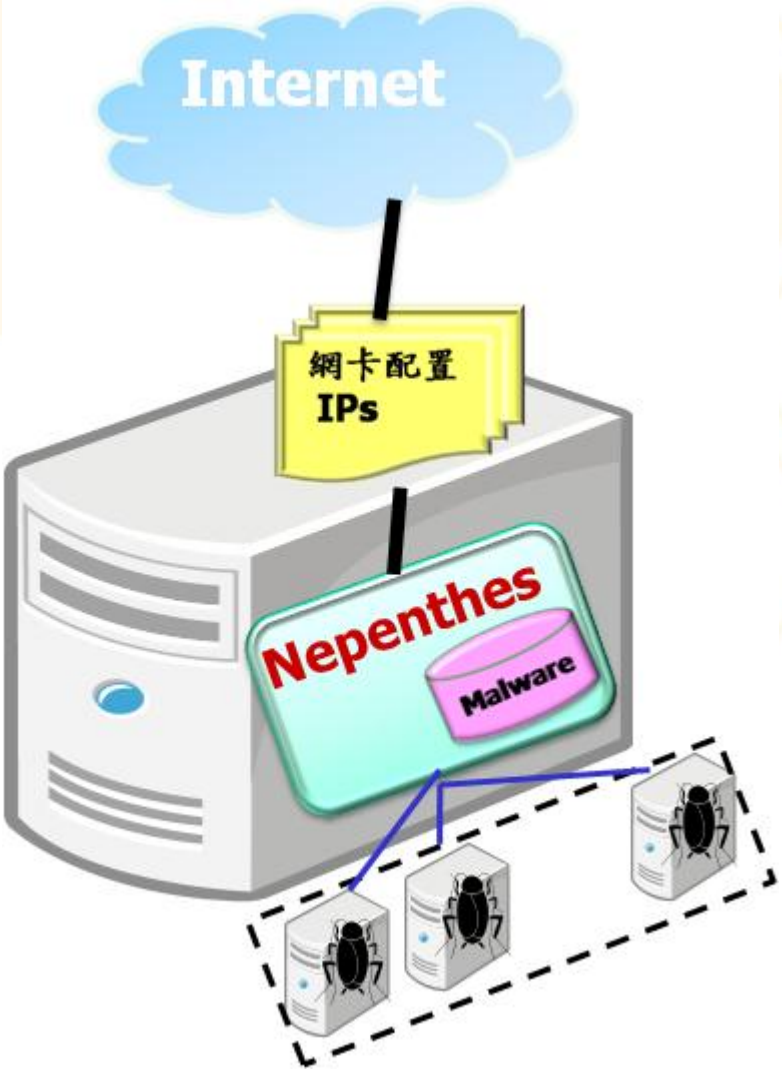
Attack under botnet

- Denial-of-service attacks : Cause target to become busy or unavailable
- Adware : Advertise some commercial entity actively and without the user‘s permission or awareness.
- Spyware: Sends information to its creators about a user's activities.
- E-mail spam: Messages are advertising, annoying, or malicious in nature.
- Click fraud : Visiting websites without the user's awareness to create false web traffic for the purpose of personal or commercial gain.
- Fast flux : Used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies.

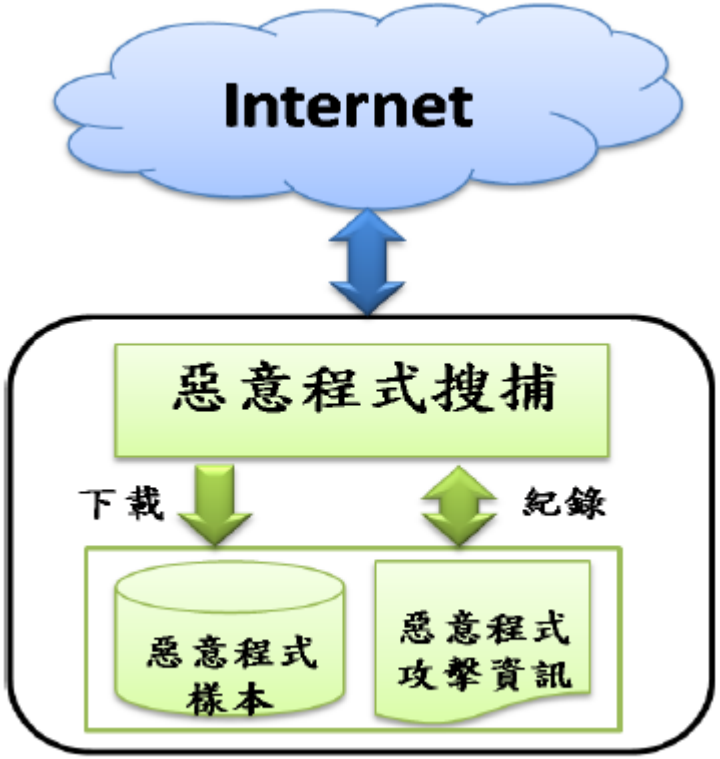
第一代惡意程式誘捕系統 -- Nepenthes

- Nepenthes 為惡意程式誘捕系統，藉由模擬系統弱點，誘使惡意程式對誘捕系統進行攻擊，進而捕捉到惡意程式 **(Autonomously Spreading)**。
  - Low-Interaction Honeypot
  - 網站: http://nepenthes.carnivore.it
  - Developer: Paul Baecher, Markus Koetter

Nepenthes Deployment (單機)

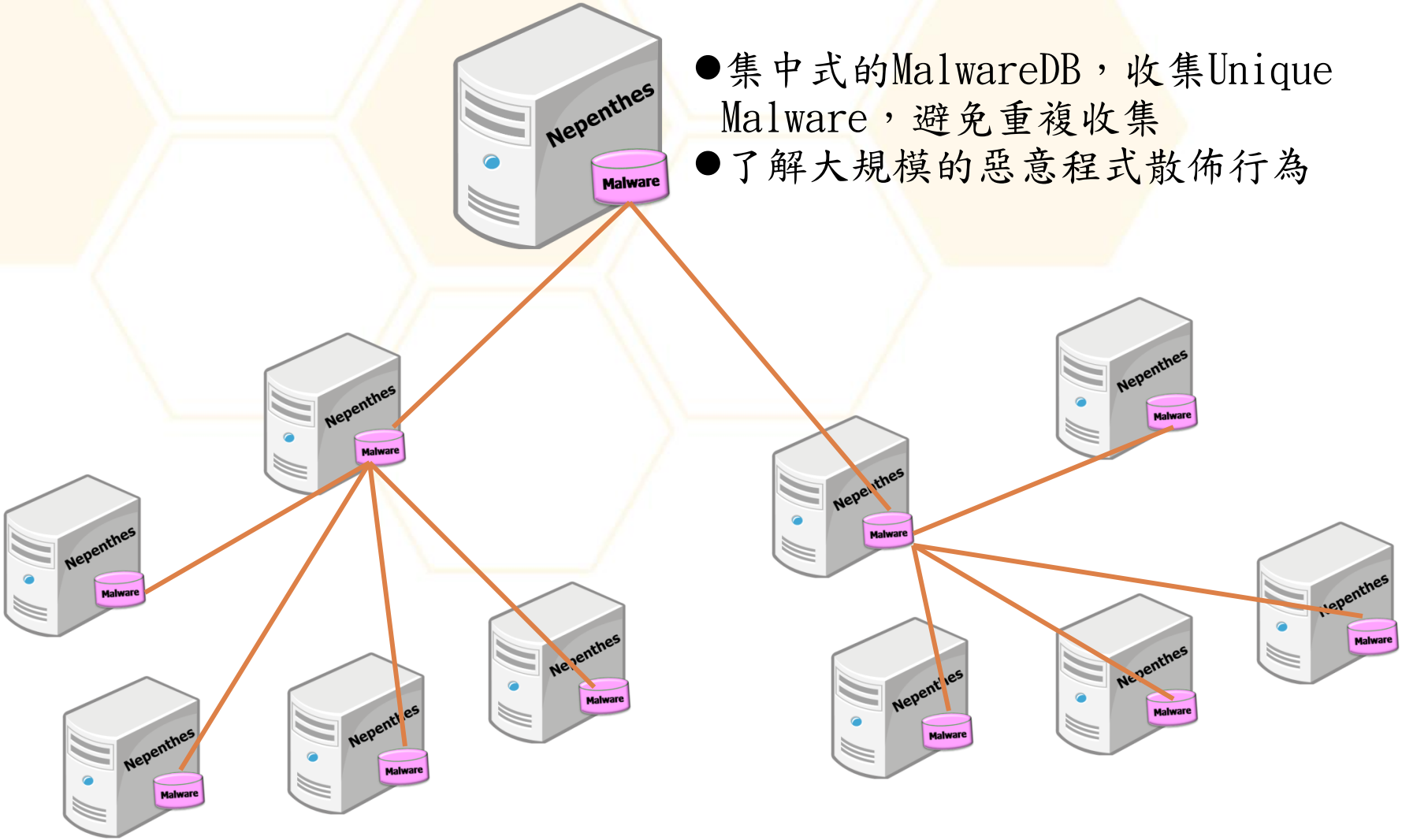


1. 準備多個IP，Bind 在同一張網卡
2. Linux-based OS上，安裝Nepenthes
3. 收集到的Malware 將會存在Disk



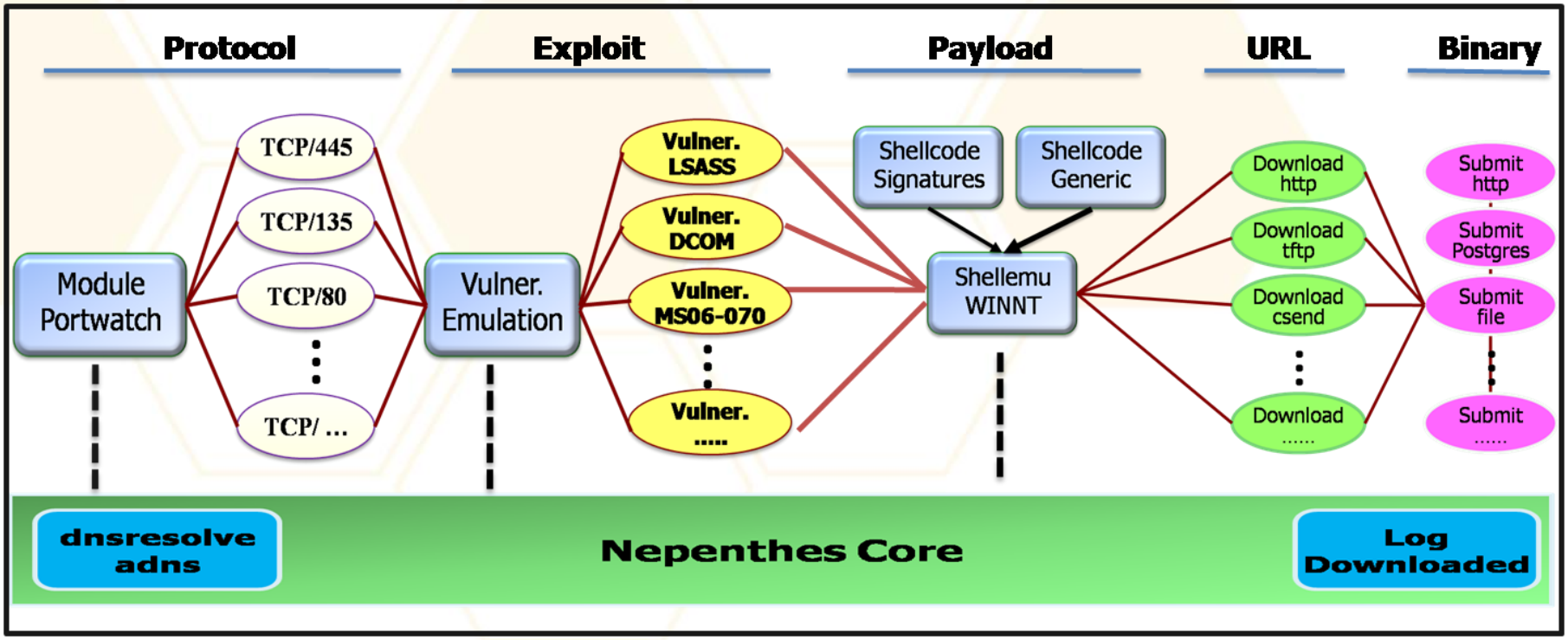
單機版惡意程式搜捕系統

Nepenthes Deployment (分散式)



- 集中式的MalwareDB，收集Unique Malware，避免重複收集
- 了解大規模的惡意程式散佈行為

Nepenthes 設計原理



- Vulnerability Modules: 模擬網路服務的弱點
- Shellcode parsing modules: 分析與反解Exploit Payload，找出Mal-URL
- Fetch Modules: 利用HTTP、FTP、TFTP…從遠端抓取惡意程式Binary
- Submission Modules: 將抓下來的惡意程式存到Disk，或其他伺服器

Nepenthes 設計原理

- Overview of Emulated Vulnerable Services

Vulnerability	Vulnerability
vuln-asn1	vuln-optix
vuln-bagle	vuln-pnp
vuln-dameware	vuln-sasserftpd
vuln-dcom	vuln-upnp
vuln-msmq	vuln-veritas
vuln-mssql	vuln-wins
vuln-mydoom	vuln-msdtc
vuln-netbiosname	vuln-ftpd
vuln-netdde	vuln-sub7
vuln-kuang2	vuln-iis
vuln-lsass	

Nepenthes安裝與設定

- OS : Ubuntu9.1.0
- 步驟:
  - Step 1. 依序編譯與安裝相依套件
  - Step 2. 安裝Nepenthes
  - Step 3. 設定與執行Nepenthes
  - Step 4. 惡意程式收集

Step 1. 依序編譯與安裝相依套件

- apt-get install libcurl3-dev libmagic-dev libpcre3-dev libadns1-dev libpcap0.8-dev iptables-dev
- apt-get install autoconfautomake1.9 autotools-dev libtool
- apt-get install subversion

Step 2. 安裝Nepenthes

- git clone git://git.carnivore.it/nepenthes.git
- cd nepenthes
- autoreconf -v -i--force
- ./configure --prefix=/opt/nepenthes
- make
- make install

Step 3. 設定與執行Nepenthes

- 設定檔: /opt/nepenthes/etc/nepenthes/nepenthes.conf
  (可採用預設，不須更動)
- 執行:/opt/nepenthes/bin/nepenthes -D

Step 3. 設定與執行Nepenthes

- 設定檔: /opt/nepenthes/etc/nepenthes/nepenthes.conf
  (可採用預設，不須更動)
- 執行:/opt/nepenthes/bin/nepenthes -D

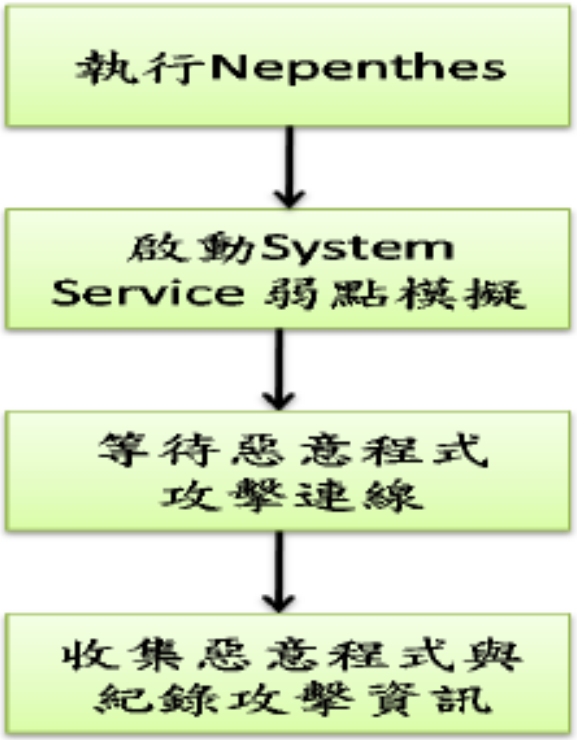
Nepenthes Files

- Nepenthes 共包含幾個重要的資料夾：
  - bin: Nepenthes執行檔
  - etc: 包含所有設定檔
  - lib: Libraries
  - share : 說明文件
  - var: 紀錄檔與惡意程式binary檔案
    - binaries
    - cache
    - hexdumps
    - log
    - spool

Step 4. 惡意程式收集

- 詳細的Log紀錄: /opt/nepenthes/var/log/nepenthes.log
- 惡意程式來源 (URL)記錄檔:
  /opt/nepenthes/var/log/logged_downloads
- 惡意程式(Binary) 下載紀錄檔:
  /opt/nepenthes/var/log/logged_submissions
- 惡意程式(Binary)儲存:
  /opt/nepenthes/var/binaries/
  以惡意程式md5值作為命名
- Exploit Code(Shellcode)儲存:
  /opt/nepenthes/var/hexdumps/

Nepenthes Functionality Testing



驗證一:Nepenthes Process執行

驗證二:開啟系統服務埠口，模擬弱點

驗證三: Testing for malware collection

驗證四:惡意程式樣本與攻擊資訊

驗證一:Nepenthes Process執行

```
roohp2@roohp2:~
[roohp2@roohp2 ~]$ ps aux|grep nepenthes
roohp2    11748  0.0  0.0   3920   680 pts/1    S+   21:17   0:00 grep nepenthes
root      26040  0.2  0.1   7544  5348 ?        Ss   Sep25  61:20 bin/nepenthes -R -D
[roohp2@roohp2 ~]$
```

驗證二:開啟系統服務埠口，模擬弱點

```
[root@roohp2 roohp2]# netstat -tnple
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       User       Inode      PID/Program name
tcp        0      0 127.0.0.1:2208              0.0.0.0:*                   LISTEN      0          12286      4694/hpiod
tcp        0      0 0.0.0.0:1025                0.0.0.0:*                   LISTEN      0          5546969    26040/nepenthes
tcp        0      0 0.0.0.0:993                 0.0.0.0:*                   LISTEN      0          5546963    26040/nepenthes
tcp        0      0 0.0.0.0:995                 0.0.0.0:*                   LISTEN      0          5546964    26040/nepenthes
tcp        0      0 0.0.0.0:3140                0.0.0.0:*                   LISTEN      0          5546980    26040/nepenthes
tcp        0      0 0.0.0.0:135                 0.0.0.0:*                   LISTEN      0          5546967    26040/nepenthes
tcp        0      0 0.0.0.0:5000                0.0.0.0:*                   LISTEN      0          5546984    26040/nepenthes
tcp        0      0 0.0.0.0:42                  0.0.0.0:*                   LISTEN      0          5546986    26040/nepenthes
tcp        0      0 0.0.0.0:139                 0.0.0.0:*                   LISTEN      0          5546979    26040/nepenthes
tcp        0      0 0.0.0.0:3372                0.0.0.0:*                   LISTEN      0          5546976    26040/nepenthes
tcp        0      0 0.0.0.0:110                 0.0.0.0:*                   LISTEN      0          5546959    26040/nepenthes
tcp        0      0 0.0.0.0:143                 0.0.0.0:*                   LISTEN      0          5546960    26040/nepenthes
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN      0          11748      4461/portmap
tcp        0      0 0.0.0.0:80                  0.0.0.0:*                   LISTEN      0          5546987    26040/nepenthes
tcp        0      0 0.0.0.0:10000               0.0.0.0:*                   LISTEN      0          5546985    26040/nepenthes
tcp        0      0 0.0.0.0:6129                0.0.0.0:*                   LISTEN      0          5546966    26040/nepenthes
tcp        0      0 0.0.0.0:465                 0.0.0.0:*                   LISTEN      0          5546962    26040/nepenthes
tcp        0      0 0.0.0.0:5554                0.0.0.0:*                   LISTEN      0          5546981    26040/nepenthes
tcp        0      0 0.0.0.0:27347               0.0.0.0:*                   LISTEN      0          5546983    26040/nepenthes
tcp        0      0 0.0.0.0:17300               0.0.0.0:*                   LISTEN      0          5546972    26040/nepenthes
tcp        0      0 0.0.0.0:21                  0.0.0.0:*                   LISTEN      0          5546970    26040/nepenthes
tcp        0      0 192.168.122.1:53            0.0.0.0:*                   LISTEN      0          13287      4956/dnsmasq
tcp        0      0 0.0.0.0:3127                0.0.0.0:*                   LISTEN      0          5546978    26040/nepenthes
tcp        0      0 0.0.0.0:2103                0.0.0.0:*                   LISTEN      0          5546973    26040/nepenthes
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN      0          12380      4725/cupsd
tcp        0      0 0.0.0.0:856                 0.0.0.0:*                   LISTEN      0          11830      4490/rpc.statd
tcp        0      0 0.0.0.0:2105                0.0.0.0:*                   LISTEN      0          5546974    26040/nepenthes
tcp        0      0 0.0.0.0:2745                0.0.0.0:*                   LISTEN      0          5546965    26040/nepenthes
tcp        0      0 0.0.0.0:25                  0.0.0.0:*                   LISTEN      0          5546958    26040/nepenthes
tcp        0      0 0.0.0.0:2107                0.0.0.0:*                   LISTEN      0          5546975    26040/nepenthes
tcp        0      0 0.0.0.0:443                 0.0.0.0:*                   LISTEN      0          5546971    26040/nepenthes
tcp        0      0 0.0.0.0:220                 0.0.0.0:*                   LISTEN      0          5546961    26040/nepenthes
tcp        0      0 0.0.0.0:445                 0.0.0.0:*                   LISTEN      0          5546968    26040/nepenthes
tcp        0      0 0.0.0.0:1023                0.0.0.0:*                   LISTEN      0          5546982    26040/nepenthes
```

驗證三：:外來惡意程式與Nepenthes互動

```
[root@roohp2 roohp2]# netstat -tvp
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
tcp        0      0 140.110.108.84:microsoft-ds client-212-117-4-108.:e-mdu SYN_RECV    -
tcp        0      0 140.110.107.59:microsoft-ds ip-189-97-227-23:facsys-ntp SYN_RECV    -
tcp        0      0 140.110.107.63:microsoft-ds 109.86.49.84:geolocate      SYN_RECV    -
tcp        0      0 140.110.108.11:microsoft-ds 187.89.190.38:net-steward   SYN_RECV    -
tcp        0      0 140.110.108.7:microsoft-ds  200165184200.user.v:ssm-cvs SYN_RECV    -
tcp        0      0 140.110.108.11:microsoft-ds 121.70.169.23:solve         SYN_RECV    -
tcp        0      1 140.110.108.11:microsoft-ds 92.81.134.87:appserv-https  FIN_WAIT1   -
tcp        0      0 140.110.108.23:microsoft-ds 189-10-238-130.pae:fj-hdnet TIME_WAIT   -
tcp        0      0 140.110.108.48:microsoft-ds adsl-160-197-182.asm.:19676 FIN_WAIT2   -
tcp        0      0 140.110.108.19:microsoft-ds 69-46-178-228.ip.to:innosys TIME_WAIT   -
tcp        0      1 140.110.108.11:microsoft-ds 59.93.200.151:ergolight     LAST_ACK    -
tcp        0      0 140.110.108.19:microsoft-ds 69-46-178-228.i:bmc-net-adm ESTABLISHED 26040/nepenthes
tcp        0      0 140.110.108.19:microsoft-ds 69-46-178-228.ip.tor.:radio TIME_WAIT   -
tcp        0      0 140.110.108.23:microsoft-ds 189-10-238-130.pae:concomp1 TIME_WAIT   -
tcp        0      0 140.110.108.13:microsoft-ds static-71-118-10-105.l:4889 TIME_WAIT   -
tcp        0      0 140.110.107.71:microsoft-ds static-188-27-8:rmiregistry ESTABLISHED 26040/nepenthes
tcp        0      0 140.110.107.56:microsoft-ds 129-089.nitka.:amt-blc-port ESTABLISHED 26040/nepenthes
tcp        0      0 140.110.108.13:microsoft-ds static-71-118-10-105.l:4667 ESTABLISHED 26040/nepenthes
tcp        0      0 140.110.107.94:microsoft-ds 194.160.28.41:4981          ESTABLISHED -
tcp        0      1 140.110.107.36:microsoft-ds static-71-102-93:solera-lpn LAST_ACK    -
tcp        0      0 140.110.107.23:microsoft-ds 79.19.182.55:4196           ESTABLISHED -
tcp        0      0 140.110.108.23:microsoft-ds 189-10-238-13:concurrent-lm TIME_WAIT   -
tcp        0      0 ::ffff:140.110.107.33:ssh   74-94-156-75-NewEngla:52384 TIME_WAIT   -
```

驗證四：：惡意程式樣本收集

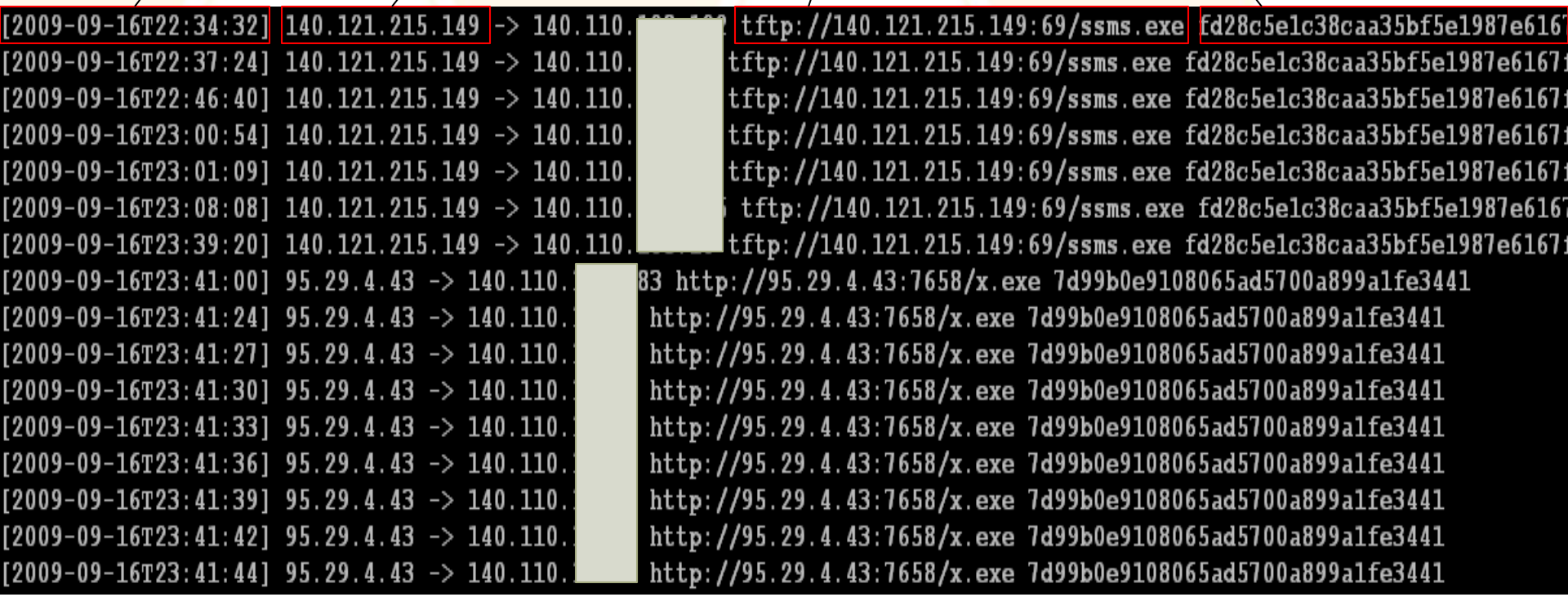
- 由/opt/nepenthes/var/binaries/ 觀看樣本資訊，樣本下載時經過md5編碼，由下圖可看出惡意程式蒐集時間與size大小
- 由下圖可看出惡意程式蒐集時間與size大小

```
-rw-r--r-- 1 root root  85K Oct  2 21:59 7b313206a2af4214b4ca00bab64e447d
-rw-r--r-- 1 root root 9.2K Sep 27 08:16 7d99b0e9108065ad5700a899a1fe3441
-rw-r--r-- 1 root root  12K Sep 29 02:20 7f60162c2c0bd2cc7531e51328e98290
-rw-r--r-- 1 root root 1.1M Sep 26 11:17 8abb75cb760379f985586d517101139f
-rw-r--r-- 1 root root 9.5K Oct  5 00:26 9716d7995acc6f6b6b90b992c4e2839d
-rw-r--r-- 1 root root 150K Sep 26 00:12 98eb0fdadf8a403c013a8b1882ec986d
-rw-r--r-- 1 root root 163K Sep 25 15:36 9a308fcc73543d9cec3a04b3d3c00220
-rw-r--r-- 1 root root 121K Oct 13 12:49 9c20944d6184d6c93edbda23a969bec8
-rw-r--r-- 1 root root 163K Sep 28 10:57 9fdc9cf56c5de858c3eaf8cc82448192
-rw-r--r-- 1 root root  46K Sep 28 04:41 a12cab51ef99e98305668d189d0db147
-rw-r--r-- 1 root root 184K Oct  8 11:42 a63dd089515bb2fe6e3a2a90800c0338
-rw-r--r-- 1 root root 1.1M Sep 27 15:24 aab88c1c5111272f07a7ad257f3673cd
-rw-r--r-- 1 root root  24K Sep 28 23:25 b26ed6eeac520491da5705ea5fb66b39
-rw-r--r-- 1 root root 9.5K Oct 11 01:53 b502f83a7c9b237018a9e24485af2b79
-rw-r--r-- 1 root root 230K Sep 26 02:38 c3b8b8e27a80f21709e0be55b2fdbd6a
-rw-r--r-- 1 root root 9.2K Sep 29 06:16 d6df3972a0ae1b094b434de0980e596c
-rw-r--r-- 1 root root 156K Sep 25 19:11 de37f2fc478495ffd5d43cb7c192a362
-rw-r--r-- 1 root root  24K Oct  3 04:53 ebddbaef33caab66200fec075fd7d601
-rw-r--r-- 1 root root  24K Oct  1 19:13 eda3b7766c23dfffc0b85d0ba546b0c1
-rw-r--r-- 1 root root  17K Oct 12 21:52 f2a8dafb3036b4bee02f31299008bc3e
-rw-r--r-- 1 root root  24K Oct 13 01:29 f59ab8529269ab771af0391148da683c
-rw-r--r-- 1 root root 149K Sep 18 09:50 fd28c5e1c38caa35bf5e1987e6167f4c
-rw-r--r-- 1 root root 121K Oct  1 01:36 fe1a007926aa37765bd8aa2d461858d6
[root@roohp2 binaries]#
```

驗證四：：惡意程式樣本收集

由/opt/nepenthes/var/log/ logged_submissions觀看攻擊資訊，

包含攻擊時間，攻擊來源IP，惡意程式存放位置，惡意程式md5



Nepenthes 的限制

- 只能收集autonomously spreading 之Malware
  (Trojan horses與rootkit，不具散佈能力無法收集)
- 無法收集browser exploits
  (需用Browser trigger，才會導致被感染)
- 只有固定幾種Windows Vulnerabilities模擬

Catch Bugs – Dionaea (捕蠅草)

- URL Link : **http://dionaea.carnivore.it**
- Authors : Markus Koetter & Mark Schloesser
- Develop from Giraffe Honeynet Project
- Dionaea : Nepenthes successor
- Trap malware exploiting vulnerabilities and the ultimate goal is gaining a copy of the malware

Dionaea Installation :

- 建議安裝於 Ubuntu Linux 作業系統
- 安裝步驟共可分為：
  - 安裝函式庫
  - 編譯Dionaea程式碼
  - 編輯Dionaea設定檔
  - 執行Dionaea
  - 觀察Dionaea記錄

Dionaea Installation -- 安裝函式庫

- aptitude install libudns-dev libglib2.0-dev libssl-dev libcurl4-openssl-dev libreadline-dev libsqlite3-dev python-dev libtool automake autoconf build-essential subversion git-core flex bison pkg-config

- apt-get install gettext
- wget http://ftp.gnome.org/pub/gnome/sources/glib/2.20/glib-2.20.4.tar.bz2
- tar xfj glib-2.20.4.tar.bz2
- cd glib-2.20.4/
- ./configure –prefix=/opt/dionaea
- make && make install
- cd ..

Dionaea Installation -- 安裝函式庫 (Cont.)

- 安裝liblcfg
  - git clone git://git.carnivore.it/liblcfg.git liblcfg
  - cd liblcfg/code
  - autoreconf -vi
  - ./configure --prefix=/opt/dionaea
  - make
  - make install
  - cd ..

Dionaea Installation -- 安裝函式庫 (Cont.)

- 安裝libemu (all)
  - git clone git://git.carnivore.it/libemu.git libemu
  - cd libemu
  - autoreconf -vi
  - ./configure --prefix=/opt/dionaea
  - make
  - make install
  - cd ..

Dionaea Installation -- 安裝函式庫 (Cont.)

- 安裝libnl (linux && optional)
  - git clone git://git.kernel.org/pub/scm/libs/netlink/libnl.git
  - cd libnl
  - autoreconf –vi
  - ./configure --prefix=/opt/dionaea
  - make
  - make install
  - cd ..

Dionaea Installation -- 安裝函式庫 (Cont.)

- 安裝libev (all)
  - wget http://dist.schmorp.de/libev/libev-3.9.tar.gz
  - tar xfz libev-3.9.tar.gz
  - cd libev-3.9
  - ./configure --prefix=/opt/dionaea
  - make
  - make install
  - cd ..

Dionaea Installation -- 安裝函式庫 (Cont.)

- Cython (all)
  - wget http://cython.org/release/Cython-0.12.1.tar.gz
  - tar xfz Cython-0.12.1.tar.gz
  - cd Cython-0.12.1
  - python setup.py build
  - python setup.py install

Dionaea Installation -- 安裝函式庫 (Cont.)

- **Python 3.1.1**
  - **readline**
    - **wget ftp://ftp.cwru.edu/pub/bash/readline-6.1.tar.gz**
    - **tar zxvf readline-6.1.tar.gz**
    - **cd readline-6.1**
    - **./configure**
    - **make**
    - **make install**
  - **sqlite > 3.3**
    - **wget http://www.sqlite.org/sqlite-amalgamation-3.7.2.tar.gz**
    - **tar zxvf** sqlite-amalgamation-3.7.2.tar.gz
    - **cd sqlite-3.7.2**
    - **./configure**
    - **make && make install**

Dionaea Installation -- 安裝函式庫 (Cont.)

- 安裝Python
  - wget http://python.org/ftp/python/3.1.2/Python-3.1.2.tgz
  - tar xfz Python-3.1.2.tgz
  - cd Python-3.1.2/
  - ./configure --enable-shared --prefix=/opt/dionaea --with-computed-gotos \
  - --enable-ipv6
  - make && make install
  - cp libpython3.1.so libpython3.1.so.1.0 /usr/lib/

Dionaea Installation -- 安裝函式庫 (Cont.)

- 安裝libxml2
  - aptitude install libxml2-dev
- 安裝libxslt
  - aptitude install libxslt1-dev
- 安裝lxml
  - wget http://codespeak.net/lxml/lxml-2.2.8.tgz
  - tar zxvf lxml-2.2.8.tgz
  - cd lxml-2.2.8
  - /opt/dionaea/bin/python3 setup.py build
  - /opt/dionaea/bin/python3 setup.py install

Dionaea Installation -- 安裝函式庫 (Cont.)

- 安裝**udns**
  - wget http://www.corpit.ru/mjt/udns/udns_0.0.9.tar.gz
  - tar xfz udns_0.0.9.tar.gz
  - cd udns-0.0.9/
  - ./configure
  - make shared
  - cp udns.h /opt/dionaea/include/
  - cp *.so* /opt/dionaea/lib/
  - cd /opt/dionaea/lib
  - ln -s libudns.so.0 libudns.so

Dionaea Installation -- 安裝函式庫 (Cont.)

- 安裝**libcurl**
  - wget http://curl.haxx.se/download/curl-7.20.0.tar.bz2
  - tar xfj curl-7.20.0.tar.bz2
  - cd curl-7.20.0
  - ./configure --prefix=/opt/dionaea
  - make && install

Dionaea Installation -- 安裝函式庫 (Cont.)

- 安裝**libpcap**
  - wget http://www.tcpdump.org/release/libpcap-1.1.1.tar.gz
  - tar xfz libpcap-1.1.1.tar.gz
  - cd libpcap-1.1.1
  - ./configure --prefix=/opt/dionaea
  - make && make install

Dionaea Installation -- 安裝函式庫 (Cont.)

- 安裝**OpenSSL (optional)(暫時先不安裝）**
  - cvs -d anonymous@cvs.openssl.org:/openssl-cvs co openssl
  - cd openssl
  - ./Configure shared --prefix=/opt/dionaea linux-x86_64
  - make SHARED_LDFLAGS=-Wl,-rpath,/opt/dionaea/lib
  - make && make install

Dionaea Compiling -- 編譯Dionaea程式碼

- git clone git://git.carnivore.it/dionaea.git dionaea
- cd dionaea
- autoreconf -vi
- ./configure --with-lcfg-include=/opt/dionaea/include/ --with-lcfg-lib=/opt/dionaea/lib/ --with-python=/opt/dionaea/bin/python3.1 --with-cython-dir=/usr/local/bin --with-udns-include=/opt/dionaea/include/ --with-udns-lib=/opt/dionaea/lib/ --with-emu-include=/opt/dionaea/include/ --with-emu-lib=/opt/dionaea/lib/ --with-gc-include=/usr/include/gc --with-ev-include=/opt/dionaea/include --with-ev-lib=/opt/dionaea/lib --with-nl-include=/opt/dionaea/include --with-nl-lib=/opt/dionaea/lib/ --with-curl-config=/opt/dionaea/bin/ --with-pcap-include=/opt/dionaea/include --with-pcap-lib=/opt/dionaea/lib/ --with-glib=/opt/dionaea
- make && make install

Dionaea Configuration – 編輯Dionaea 設定檔

- 設定檔置於：/opt/dionaea/etc/dionaea/dionaea.conf
- Dionaea.conf 為主程式重要設定檔，共包含六個部分：
  - Logging：用於指定log domains and loglevel
  - Processors：用於控制 emu processor偵測Shellcode，並送出回應(Bi-directional Streams)
  - Downloads: 指定惡意程式儲存位置
  - Bistreams：儲存Bi-directional Streams
  - Submit：利用 HTTP或FTP轉存惡意程式樣，如：利用FTP
  - Listen: 指定Dionaea監控IP，預設是All，亦即所有惡意程式連線都會被抓取
  - Modules：指定各種模擬

Dionaea Configuration – 編輯Dionaea 設定檔 (Cont.)

- Dionaea.conf 中，Modules 設定檔說明：
  - Pcap module：採用Libpcap 函式庫來記錄與偵測 Rejected Connection Attempts，來獲得攻擊來源資訊
  - Curl module : Curl模組被使用於傳送檔案到第三方伺服器
  - Emu module: 偵測、執行與解析Shellcode
  - Python module: 利用Python interpreter來控制Dionaea
  - Logsql module: 將Dionaea Log資訊儲存到sqlite databse中
  - Logxmpp module: 將Dionaea Log資訊儲存到xmpp server
  - P0f module: 提供攻擊來源 OS fingerprinting功能

Running Dionaea – 執行Dionaea

- 執行參數：
  - -c, --config=FILE (設定檔位置)
  - -D, (背景執行)
  - -g, --group=GROUP (switch to GROUP after startup)
  - -h, --help display help
  - -H, --large-help
  - -l, --log-levels="all, debug, info, message, warning, critical"
  - -u, --user=USER (switch to USER after startup)
  - -p, --pid-file=FILE (write pid to file)
  - -r, --chroot=DIR (chroot to DIR after startup)
  - -V, (show version)
  - -w, --workingdir=DIR (set the process working dir to DIR)
- 執行命令：dionaea -u nobody -g nogroup -r /opt/dionaea/ -w /opt/dionaea -p /opt/dionaea/var/dionaea.pid –D

惡意程式分析:線上病毒掃描

- **Kaspersky Virus File Scanner**
  - http://www.kaspersky.com/scanforvirus
- **Dr.Web ® online check**
  - http://online.us.drweb.com/
- **avast! Online Scanner**
  - http://onlinescan.avast.com/
- **ClamAV Online Specimen Scanner**
  - http://www.gietl.com/test-clamav/

惡意程式分析:線上病毒掃描(Cont.)

- **Online Virus Scanner & Submission**
  - http://www.fortiguardcenter.com/antivirus/virus_scanner.html
- **ThreatExpert – Online File Scanner**
  - http://www.threatexpert.com/filescan.aspx
- **VirusTotal – 免費線上病毒和惡意軟體掃瞄**
  - http://www.virustotal.com/zh-tw/
- **Jotti Online malware scan**
  - http://virusscan.jotti.org/

惡意程式分析:線上病毒掃描(Cont.)

- **Virus.Org :: Malware Scanning**
  - http://scanner.virus.org/
- **VirSCAN.org-線上防毒引擎掃瞄網站 (使用 39 種防毒軟體掃瞄引擎)**
  - http://www.virscan.org/
- **Filterbit (使用 8 種防毒軟體掃瞄引擎)**
  - http://www.filterbit.com/

惡意程式分析:線上病毒掃描(Cont.)

- **ThreatExpert: 線上行為分析與檢測工具**
  - http://www.threatexpert.com/submit.aspx
- **Sunbelt CWSandbox**
  - http://www.sunbeltsecurity.com/Submit.aspx
- **Anubis: Analyzing Unknown Binaries**
  - http://anubis.iseclab.org/
- **Norman Sandbox**
  - http://www.norman.com/security_center/security_tools/submit_file/en

惡意程式分析工具

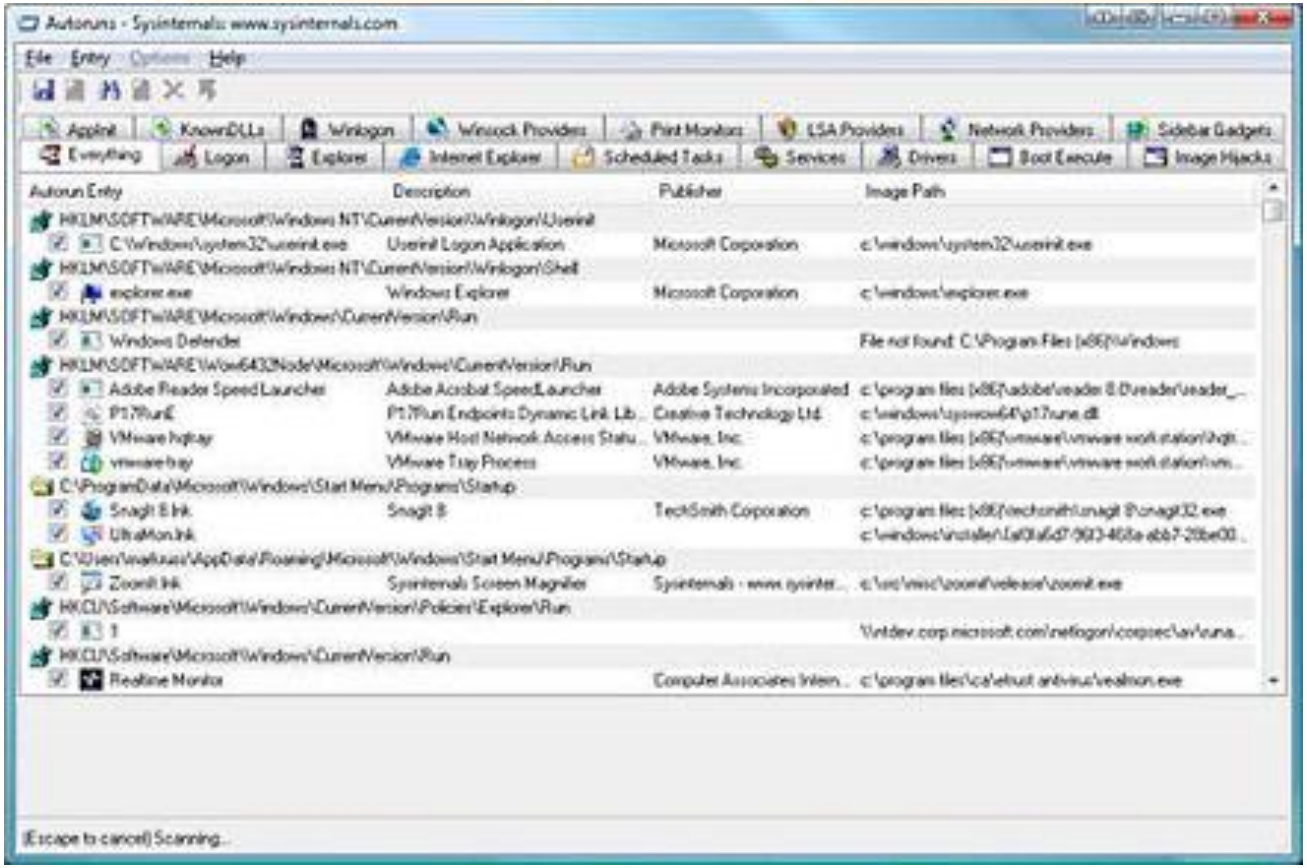
- 目的: **協助分析人員找出電腦異常的可疑原因**，如: 未經Verfied 檔案，不正常大量網路連線，可疑啟動項目，可疑的系統服務，可疑的處理程。
- 分析工具分類:
  - 系統監控: **收集受感染Process、DLL、File、Registry、Service資訊提**供分析，
  - 網路監控: **監控該電腦即時的網路連線與程序執行狀態，做為攻擊分**析之依據

惡意程式分析工具-系統監控

- Autoruns
- Procexp (Process Explorer)
- TCPView
- System Repair Engineer(SREng)

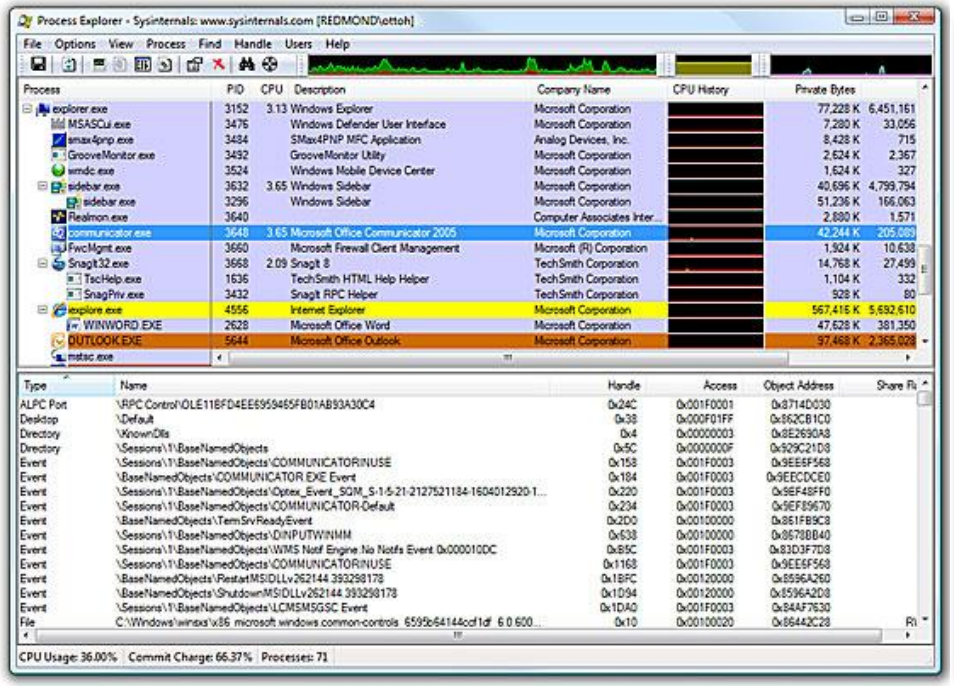
惡意程式分析工具-Autoruns

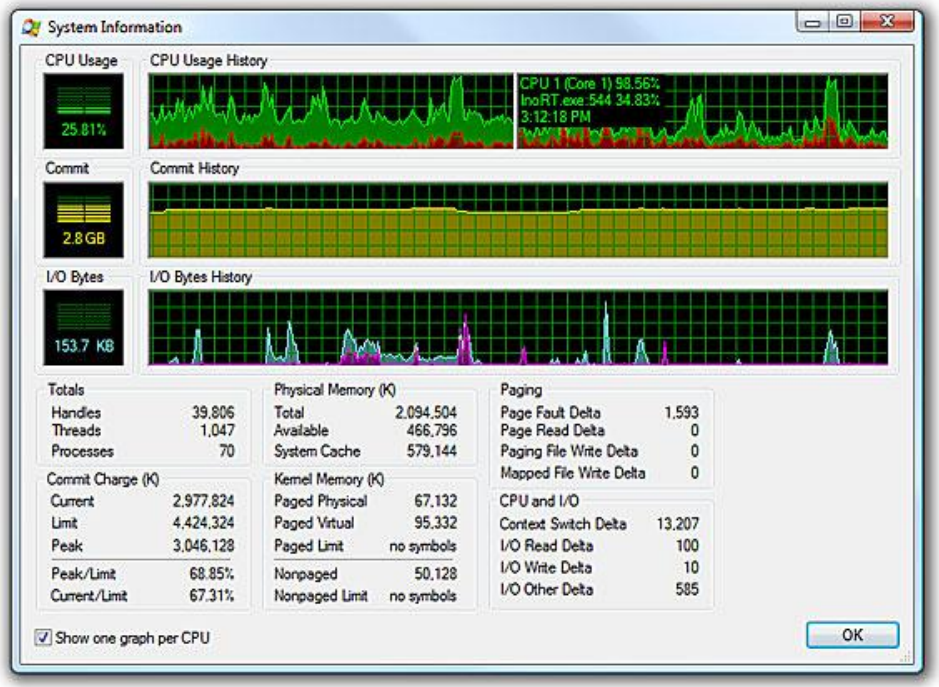
- **Autoruns：檢查有哪些程式在一開機就自動執行，快速的檢查啟動項目**
  - http://download.sysinternals.com/Files/Autoruns.zip



Procexp (Process Explorer)

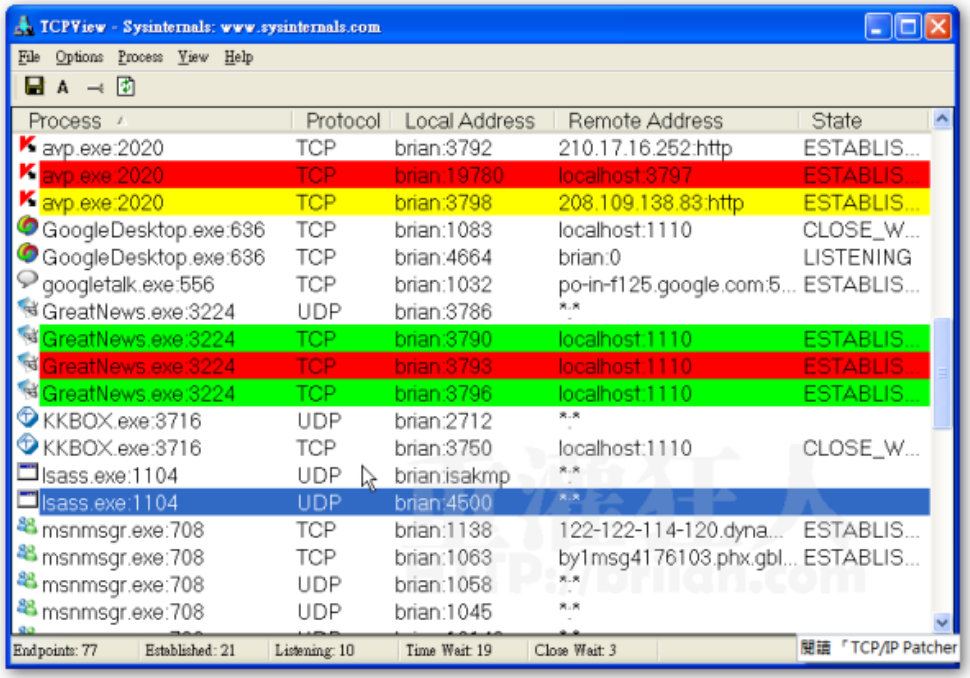
- **Procexp (Process Explorer): 類似windows工作管理員，Sysinternals**開發免費工具，檢視系統執行程序與相關即時資訊及存檔，刪除、暫停、重新啟動執行程序與除錯，調整執行程序優先權，線上查詢執行程序相關資訊，調整執行程式的使用者權限
  - http://download.sysinternals.com/Files/ProcessExplorer.zip





TCPView

- **Tcpview: 微軟提供的一個很方便的小工具，主要功能就是列出本機電腦**的全部對外連線狀況，可監控電腦上 TCP 及 UDP 連線情況的圖形化工具軟體，其能顯示所有進出系統的連線資訊，包括連線的程序、協定、本機及遠端位址、連線狀態等
  - http://download.sysinternals.com/Files/tcpview.zip



System Repair Engineer(SREng)

- **SREng: KZTechs.com網站作者Samllfrogs開發免費工具，收集系統資訊，**系統維護與修復，主要診斷未經簽署的程序與被修改的登錄資訊，資訊較少約15至40kb，分析簡易迅速
  - hKp://www.kztechs.com/sreng/download.html