有關 DNS 查詢惡意網域的處理方式，感謝臺中市教育網路中心劉育彰老師提供的處理方式，供各位參考：

設定防止 DNS 查詢特殊網域及分析 log

臺中市教育網路中心 黃國順

2013/11/12

下面使用 CentOS 來示範

軟體: BIND

1. 修改 named.conf (紅色部分請修改為符合自己學校的內容)

```
#vi /var/named/chroot/etc/named.conf
```

1-1.在 options 段加入允許遞迴查詢的網段(部分版本較舊的 BIND 不支援此功能)

```
options {
        allow-recursion { 127.0.0.1/32; 192.168.x.0/24; 140.128.x.0/24;
2001:288:52xx::/48; };
  };
```

1-2. 加入想要阻擋的特殊「網址名稱」(目前有 5 個，未來若還有會增加)

```
zone "world.rickstudio.ru" { type master; file "dummy-block"; };
zone "juice.losmibracala.org" { type master; file "dummy-block"; };
zone "web1.51.la" { type master; file "dummy-block"; };
zone "murik.portal-protection.net.ru" { type master; file "dummy-block"; };
zone "slade.safehousenumber.com" { type master; file "dummy-block"; };
zone "test.com" { type master; file "dummy-block"; };
```

【註: 最後一個 test.com 是為了測試才加入，測試後請刪除。】

1-3. 為了找出有問題的電腦 IP 要加入 logging 段

```
logging {
              channel default-log {
                            file "/var/log/default-log" versions 10 size 20m;
                            severity info;
                              print-time yes;
              };

              channel lamer-log {
                            file "/var/log/lamer-log" versions 3 size 10m;
                            severity info;
```

```
                print-severity yes;
                  print-time yes;
                print-category yes;
        };

        channel query-log {
                file "/var/log/query-log" versions 10 size 10m;
                severity info;
                  print-time yes;
        };

        channel security-log {
                file "/var/log/security-log" versions 3 size 1m;
                severity info;
                print-severity yes;
                  print-time yes;
                print-category yes;
        };

        category lame-servers { lamer-log; };
        category security{ security-log;};
        category queries { query-log;};
          category default {default-log;};
 };
```

2. 新增 dummy-block 檔案

#vi /var/named/chroot/var/named/dummy-block

內容如下(紅色部分請修改為自己學校的內容):

```
$TTL 24h

@       IN SOA server.xxes.tc.edu.tw. hostmaster.xxes.tc.edu.tw. (20131110    86400
300    604800    3600 )

@       IN      NS      server.xxes.tc.edu.tw.
@       IN      A       127.0.0.1
*       IN      A       127.0.0.1
```

3. 重新啟動 named 及測試

#service named restart

```
#nslookup
>test.com
Name:     test.com
Address: 127.0.0.1
```

若 test.com 回應為 127.0.0.1 便是有效了。

4. 查詢是否能正常產生 query-log

```
#ls -la /var/named/chroot/var/log
drwxrwx--- 2 named named         4096 11 月  10 22:30 .
drwxr-x--- 6 root    named         4096    9 月    9 12:01 ..
-rw-r--r-- 1 named named      887182 11 月  10 22:13 default-log
-rw-r--r-- 1 named named    2531058 11 月  10 22:36 lamer-log
-rw-r--r-- 1 named named 15233110 11 月  10 22:38 query-log
-rw-r--r-- 1 named named         2282 11 月  10 03:01 security-log
```

5. 新增分析程式 /root/filter.sh

內容如下

```
#!/bin/bash

# search_path 參數為 BIND log 存放路徑
search_path=/var/named/chroot/var/log


test -e $search_path/filter-result || touch $search_path/filter-result
test -e $search_path/filter-result-temp || touch $search_path/filter-result-temp

for FILENAME in $(find $search_path -mmin -10 -name 'query-*' -print | sed 's/^\.\///');
do

IFS=","
export IFS;
#要過濾的特殊網址請加在 words 參數中，並以「,」隔開
words="juice.losmibracala.org,web1.51.la,world.rickstudio.ru,webimg.51.la,slade.safeho
usenumber.com"
#    echo $FILENAME
   for word in $words; do
     grep $word $FILENAME >>    $search_path/filter-result-temp
   done
done
```

```
sort $search_path/filter-result-temp > $search_path/filter-result-temp2
mv $search_path/filter-result-temp2 $search_path/filter-result-temp
comm -2 -3 $search_path/filter-result-temp    $search_path/filter-result >
$search_path/filter-result-mail
cat $search_path/filter-result-mail >> $search_path/filter-result
rm -f $search_path/filter-result-temp
```

6. 設定 filter.sh 具有執行權並測試

```
#chmod +x filter.sh
#/root/filter.sh
```

7. 查看過濾結果 filter-result

```
#cat /var/named/chroot/var/log/filter-result
```

內容格式如下:

```
08-Nov-2013 10:30:52.012 client 163.17.x.y#61440: query: web1.51.la IN A +
(163.17.a.b)
```

這樣我們就可以找出有問題的 IP 了: 163.17.x.y

8. 設定 crontab 每 10 分鐘定時執行 filter.sh 一次

```
#crontab -e
```

加入下面這一行

```
*/10 * * * * /root/filter.sh
```