```
Client: PASS $!0@
Client: NICK [NIP]-IBM6N4SKA
Client: USER YSNARFAL "ask0.org" "FCK" :YSNARFAL

Server: :leaf.4714.com 001 [NIP]-IBM6N4SKA :BBNet, [NIP]-IBM6N4SKA!
YSNARFAL@114-30-XXX-XX.ip.adam.com.au

Server: :leaf.4714.com 005 [NIP]-IBM6N4SKA MAP KNOCK SAFELIST HCN
MAXCHANNELS=10 MAXBANS=60 NICKLEN=30 TOPICLEN=307 KICKLEN=307
MAXTARGETS=15 AWAYLEN=307 :are supported by this server

Server: :leaf.4714.com 005 [NIP]-IBM6N4SKA WALLCHOPS WATCH=128 SILENCE=15
MODES=12 CHANTYPES=# PREFIX=(qaohv)~&@%+
CHANMODES=be,kfL,l,psmntirRcOAQKVGCuzNSMT NETWORK=BBNet CASEMAPPING=ascii
EXTBAN=~,cqr :are supported by this server

Server: :[NIP]-IBM6N4SKA MODE [NIP]-IBM6N4SKA :+i

Server: PING :leaf.4714.com

Client: PONG leaf.4714.com
```

```
Client: JOIN #mipsel %#8b

Server: :[NIP]-IBM6N4SKA!YSNARFAL@114-30-XXX-XX.ip.adam.com.au JOIN
:#mipsel

Server: :leaf.4714.com 332 [NIP]-IBM6N4SKA #mipsel :.silent on .killall
.lscan .rlscan .esel [US],[FR],[IT],[GB],[ES],[DE] rejoin 10800 10800

Server: :leaf.4714.com 333 [NIP]-IBM6N4SKA #mipsel DRS 1228994845

Server: :leaf.4714.com 353 [NIP]-IBM6N4SKA @ #mipsel :[NIP]-IBM6N4SKA

Server: :leaf.4714.com 366 [NIP]-IBM6N4SKA #mipsel :End of /NAMES list.
```

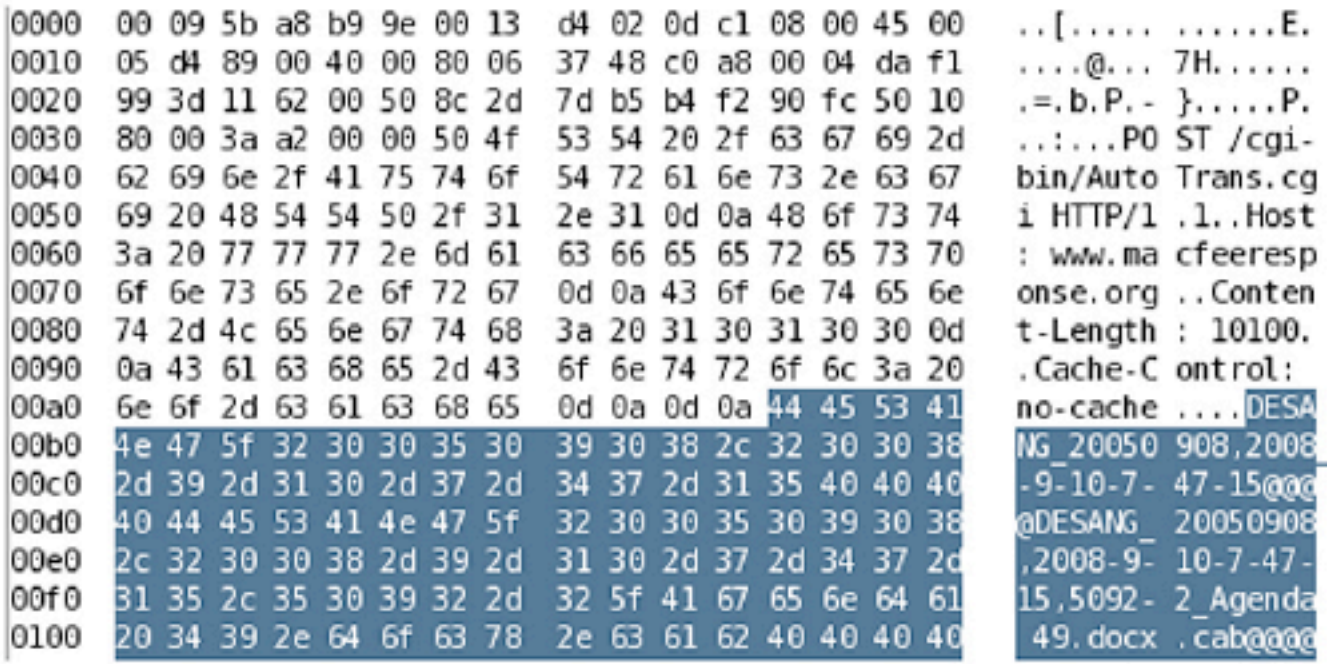
```
.visit              - flood URL with GET requests
.scan                    - scans a random range for vulnerable routers/modems
.rscan            - scans a CIDR range for vulnerable routers/modems
.lscan                   - scans the local subnet for vulnerable routers/modems
.lrscan                  - scans a range in the local subnet for vulnerable routers/modems
.split         - splits the workload of a scan thread into two threads
.sql         - scans for vulnerable MySQL servers and attempts to make them download and run URL
.pma         - scans for vulnerable phpMyAdmin and attempts to make them download and run URL
.sleep             - makes the bot sleep for the given time
.sel                     - ???
.esel                    - skip next part if locale is not X
.vsel                    - skip next part if version is not X
.gsel                    - ???
.rejoin [delay]          - cycle the channel after delay
.upgrade                 - download new bot from the distribution site
```

It appears that Netcomm NB5 ADSL modems are not the only devices affected by this bot.

Modems with similar hardware configurations (unknown brands) from Italy, Brazil, Ecuador, Russia, Ukraine, Turkey, Peru, Malaysia, Columbia, India and Egypt (and likely more countries) also seem to be affected, and are spreading the bot.

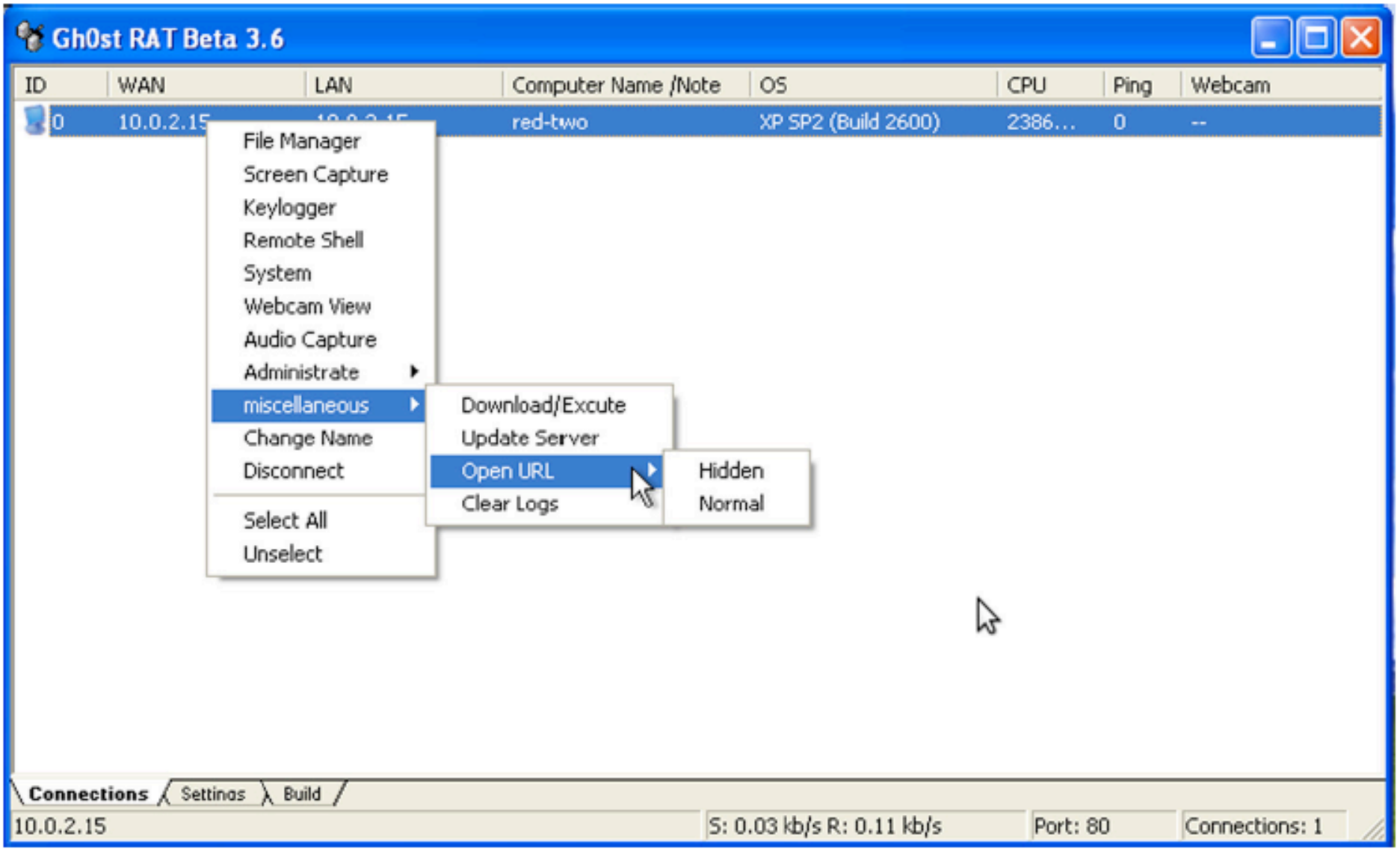
Introduction:

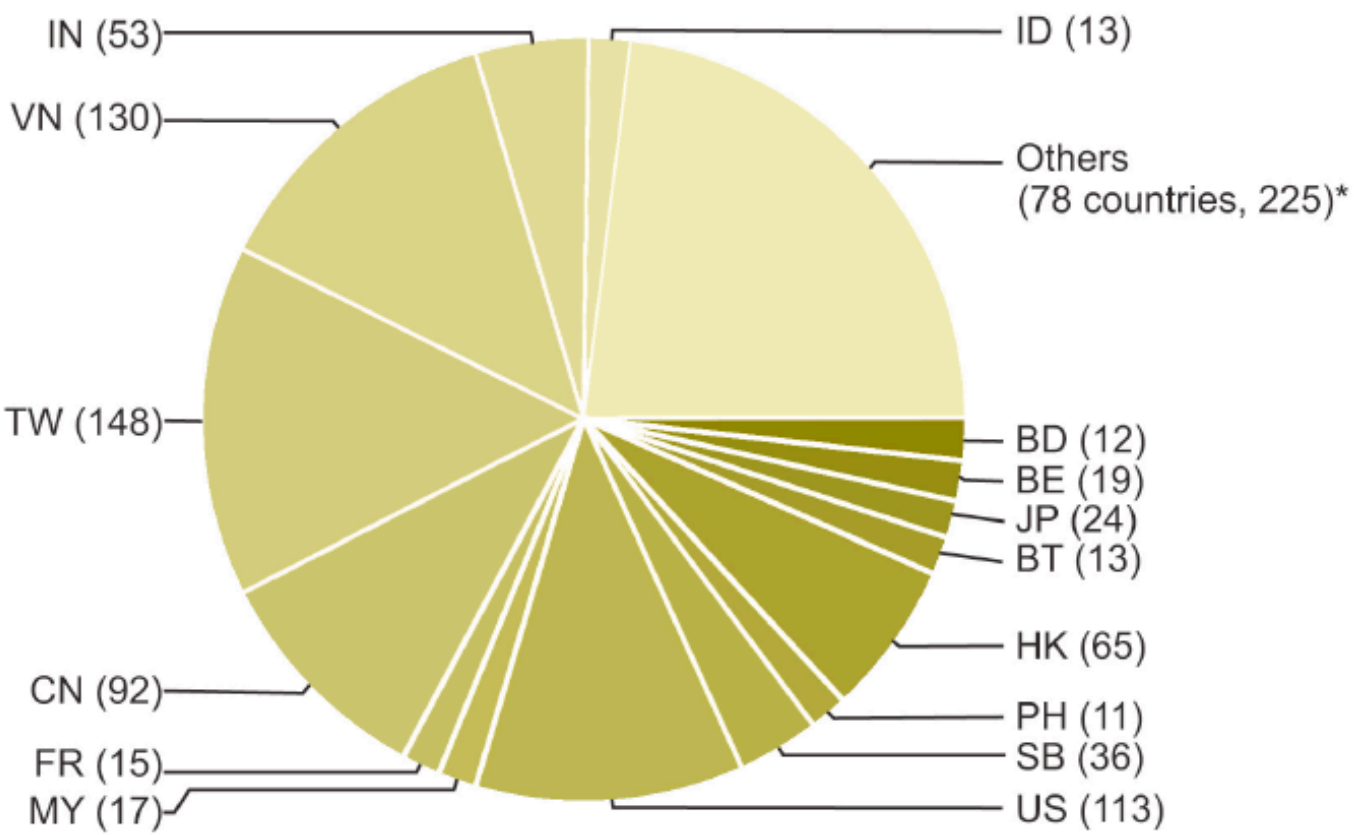
The NB5 was a popular ADSL/ADSL2+ modem-router, produced by Netcomm circa 2005. The NB5 is based on the Texas Instruments TNETD7300, featuring a 32bit RISC MIPS 4KEc V4.8 processor, 2MB of flash ROM, 8MB of RAM, Ethernet + USB connectivity, and runs an embedded Linux distribution.



```
0000  00 09 5b a8 b9 9e 00 13  d4 02 0d c1 08 00 45 00   ..[..... ......E.
0010  05 d4 89 00 40 00 80 06  37 48 c0 a8 00 04 da f1   ....@... 7H......
0020  99 3d 11 62 00 50 8c 2d  7d b5 b4 f2 90 fc 50 10   .=.b.P.- }.....P.
0030  80 00 3a a2 00 00 50 4f  53 54 20 2f 63 67 69 2d   ..:...PO ST /cgi-
0040  62 69 6e 2f 41 75 74 6f  54 72 61 6e 73 2e 63 67   bin/Auto Trans.cg
0050  69 20 48 54 54 50 2f 31  2e 31 0d 0a 48 6f 73 74   i HTTP/1 .1..Host
0060  3a 20 77 77 77 2e 6d 61  63 66 65 65 72 65 73 70   : www.ma cfeeresp
0070  6f 6e 73 65 2e 6f 72 67  0d 0a 43 6f 6e 74 65 6e   onse.org ..Conten
0080  74 2d 4c 65 6e 67 74 68  3a 20 31 30 31 30 30 0d   t-Length : 10100.
0090  0a 43 61 63 68 65 2d 43  6f 6e 74 72 6f 6c 3a 20   .Cache-C ontrol:
00a0  6e 6f 2d 63 61 63 68 65  0d 0a 0d 0a 44 45 53 41   no-cache ....DESA
00b0  4e 47 5f 32 30 30 35 30  39 30 38 2c 32 30 30 38   NG_20050 908,2008
00c0  2d 39 2d 31 30 2d 37 2d  34 37 2d 31 35 40 40 40   -9-10-7- 47-15@@@
00d0  40 44 45 53 41 4e 47 5f  32 30 30 35 30 39 30 38   @DESANG_ 20050908
00e0  2c 32 30 30 38 2d 39 2d  31 30 2d 37 2d 34 37 2d   ,2008-9- 10-7-47-
00f0  31 35 2c 35 30 39 32 2d  32 5f 41 67 65 6e 64 61   15,5092- 2_Agenda
0100  20 34 39 2e 64 6f 63 78  2e 63 61 62 40 40 40 40    49.docx .cab@@@@
```

The attacker exfiltrates a MS Word document that contains details of the Dalai Lama's negotiating position


Gh0st RAT Beta 3.6
ID
WAN
LAN
Computer Name /Note
OS
CPU
Ping
Webcam
0
10.0.2.15
red-two
XP SP2 (Build 2600)
2386...
0
--
File Manager
Screen Capture
Keylogger
Remote Shell
System
Webcam View
Audio Capture
Administrate
miscellaneous
Change Name
Disconnect
Select All
Unselect
Download/Excute
Update Server
Open URL
Clear Logs
Hidden
Normal
Connections
Settings
Build
10.0.2.15
S: 0.03 kb/s R: 0.11 kb/s
Port: 80
Connections: 1

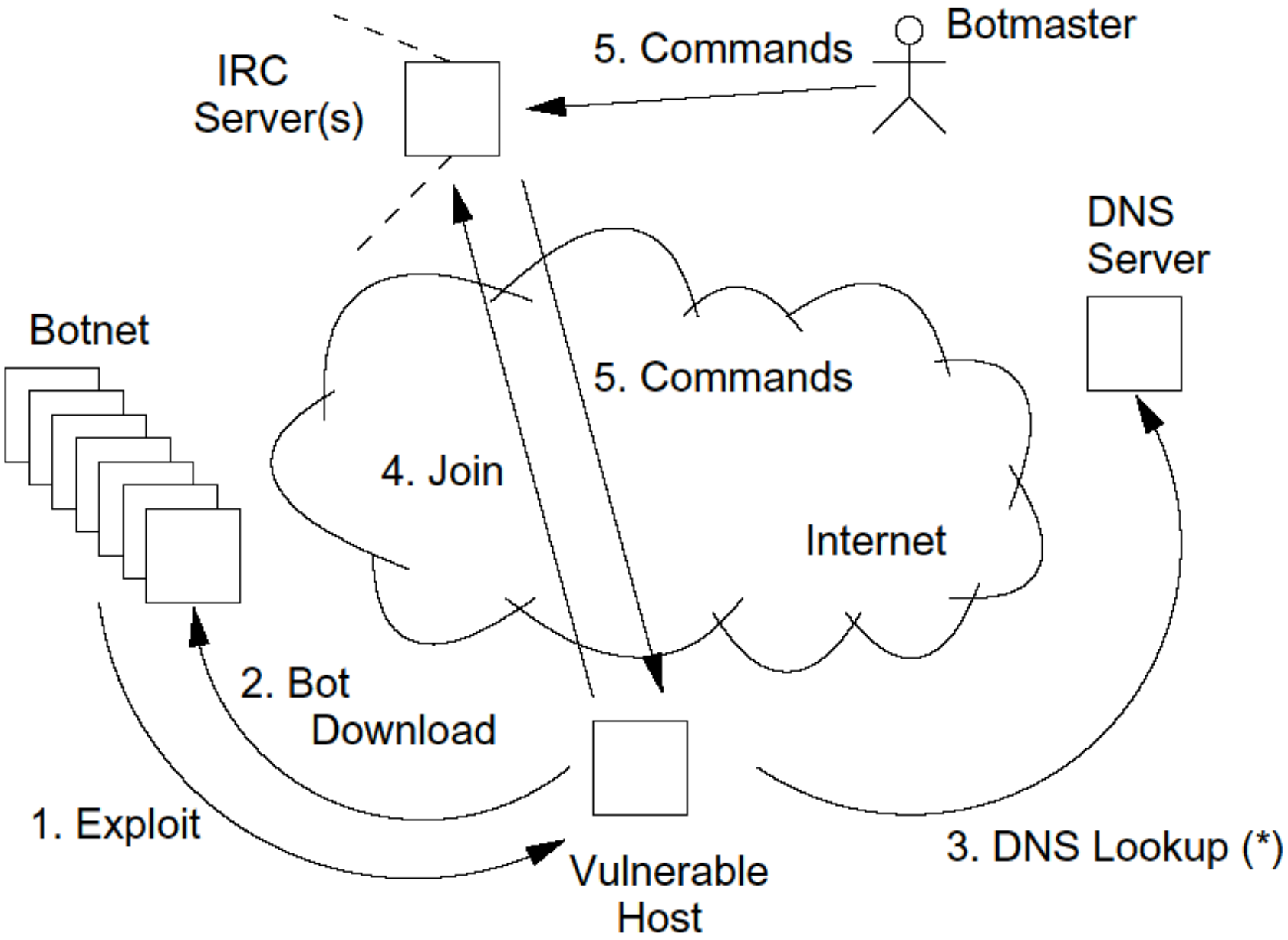


COUNTRY KEY

IN	India
VN	Vietnam
TW	Taiwan
CN	China
FR	France
MY	Malaysia
ID	Indonesia
BD	Bangladesh
BE	Belgium
JP	Japan
BT	Bhutan
HK	Hong Kong
PH	Philippines
SB	Soloman Islands
US	USA

Table 2: Selected infections

Organization	Confidence	Location	Infections
ASEAN	H	ID, MY	3
Asian Development Bank	H	PH, IN	3
Associated Press, UK	H	GB, HK	2
Bureau of International Trade Relations	L	PH	1
CanTV, Venezuela	H	VE	8
Ceger, Portugal	H	PT	1
Consulate General of Malaysia, Hong Kong	H	HK	1
Embassy Of India, Kuwait	H	KW	1
Embassy of India, USA	H	US	7
Embassy of India, Zimbabwe	H	ZA	1
Embassy of Indonesia, China	H	CN	1
Embassy of Malaysia, Cuba	H	CU	1
Embassy of Malaysia, Italy	H	IT	1
Ministry of Industry and Trade, Vietnam	L	VN	30
Ministry of Labour and Human Resources, Bhutan	H	BT	1
National Informatics Centre, India	L	IN	12
NATO, (SHAPE HQ)	H	NL	1
Net Trade, Taiwan	H	TW	1
New Tang Dynasty Television, United States	L	US	1
Office of the Dalai Lama, India	H	IN	2


IRC
Server(s)
5. Commands
Botmaster
DNS
Server
Botnet
5. Commands
4. Join
Internet
2. Bot
Download
1. Exploit
Vulnerable
Host
3. DNS Lookup (*)

Security Fix

Brian Krebs on Computer Security

SEARCH THIS BLOG

Go

RECENT POSTS

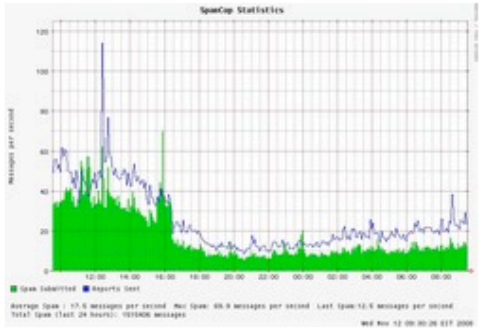
- E-Banking on a Locked Down PC, Part II
- ChoicePoint Breach Exposed 13,750 Consumer Records
- President Obama on Cyber Security Awareness
- Mozilla Disables Microsoft's Insecure Firefox Add-on
- PayChoice Suffers Another Data Breach

Entries By Category

- Cyber Justice
- Economy Watch
- Fraud
- From the Bunker
- Latest Warnings
- Misc.
- New Patches
- Piracy
- Safety Tips

Spam Volumes Drop by Two-Thirds After Firm Goes Offline

The volume of junk e-mail sent worldwide plummeted on Tuesday after a Web hosting firm identified by the computer security community as a major host of organizations engaged in spam activity was taken offline. (**Note**: A link to the full story on McColo's demise is available here.)



Experts say the precipitous drop-off in spam comes from Internet providers unplugging **McColo Corp.**, a hosting provider in Northern California that was the home base for machines responsible for coordinating the sending of roughly 75 percent of all spam each day.

In an alert sent out Wednesday morning, e-mail security firm **IronPort** said:

> In the afternoon of Tuesday 11/11, IronPort saw a drop of almost 2/3 of overall spam volume, correlating with a drop in IronPort's SenderBase queries. While we investigated what we thought might be a technical problem, a major spam network, McColo Corp., was shutdown, as reported by The Washington Post on Tuesday evening.

Spamcop.net's graphic shows a similar decline, from about 40 spam e-

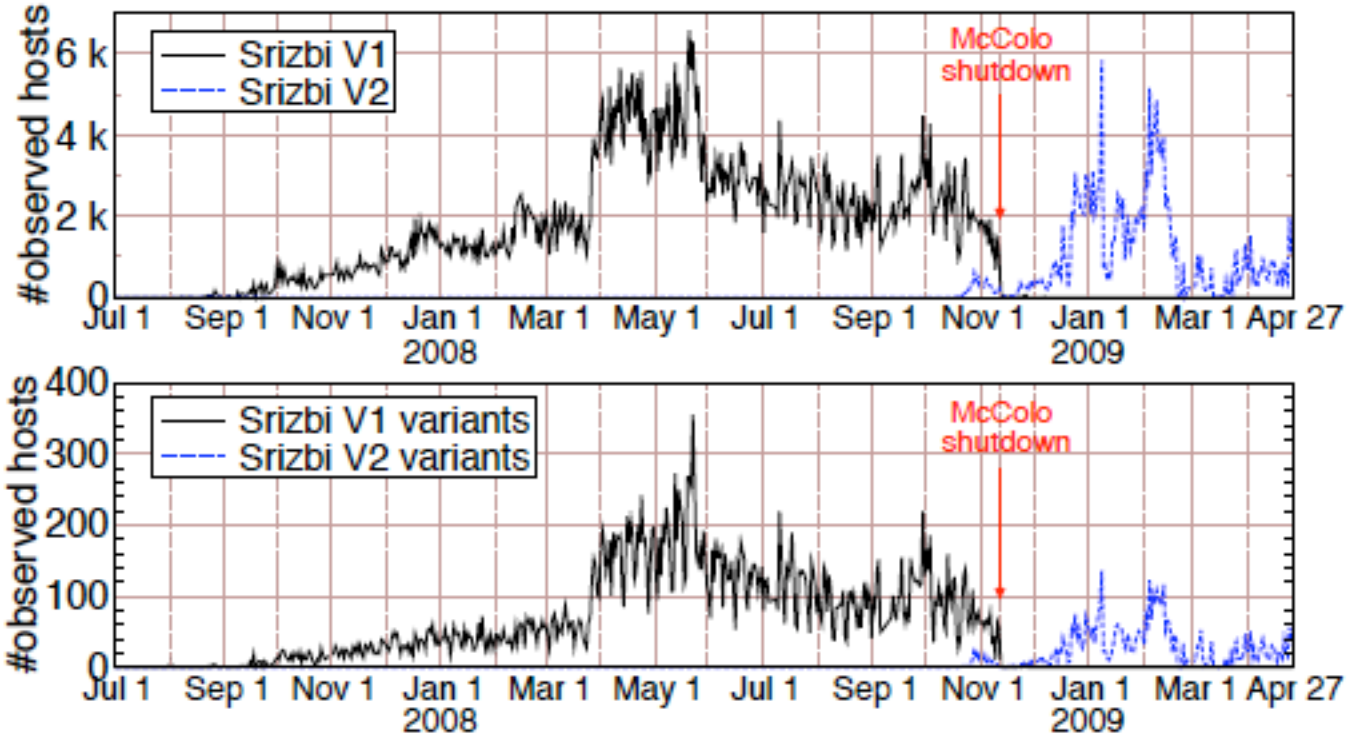
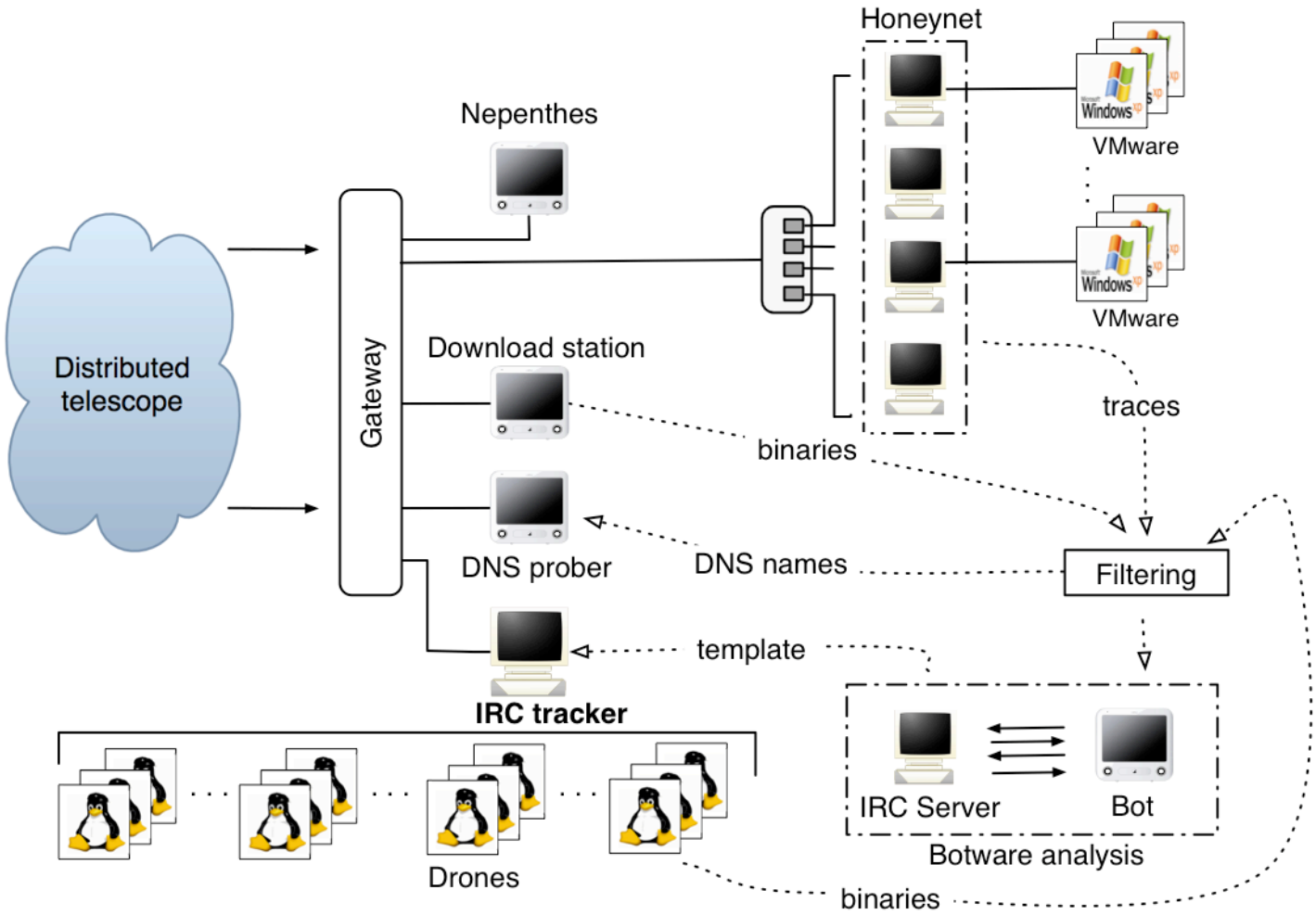


Figure 3: Number of observed hosts infected with Srizbi V1/V2 (top) and their variants (bottom) in the MAWI data set.


Honeynet
Nepenthes
VMware
VMware
Distributed telescope
Gateway
Download station
traces
binaries
DNS prober
DNS names
Filtering
template
IRC tracker
IRC Server
Bot
Botware analysis
Drones
binaries

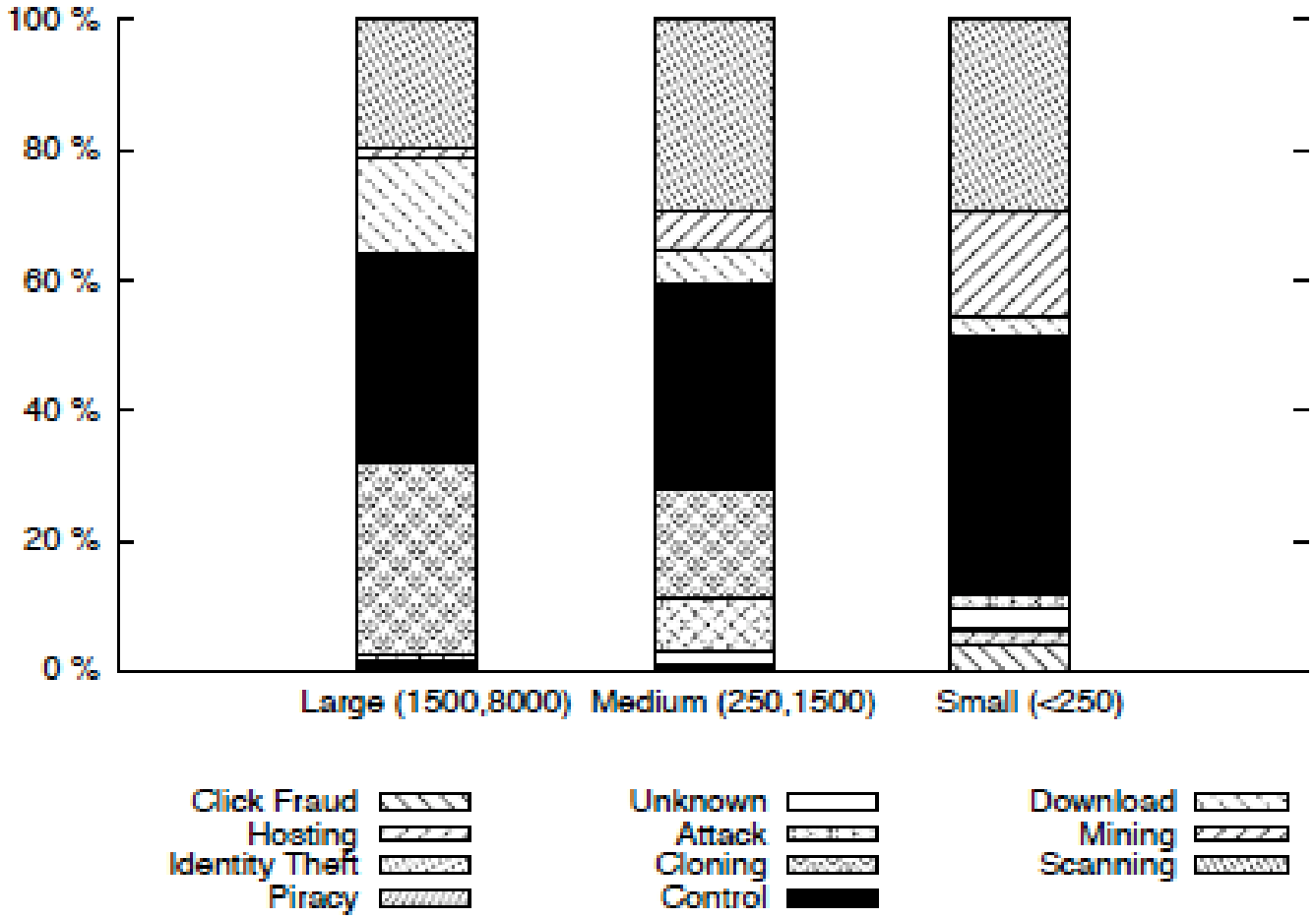
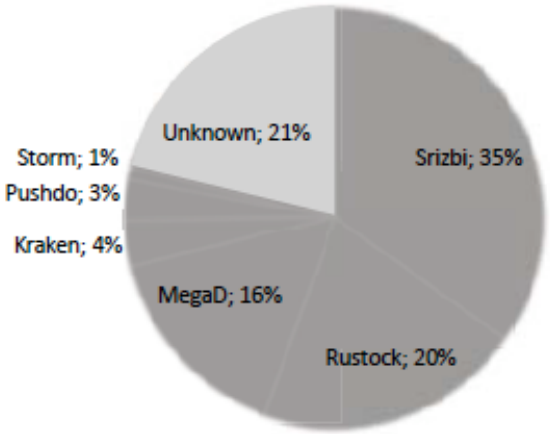


Figure 13: Percentage of command types as a function of observed botnet size.

Botnet	# days active in trace	total spam messages	spam send rate (messages/min)	C&C protocol	C&C servers contacted over lifetime	C&C discovery
Grum	8 days	864,316	344	encrypted HTTP, port 80	1	static IP (206.51.231.192)
Kraken	25 days	5,046,803	331	encrypted HTTP, port 80	41	algorithmic DNS lookups
Pushdo	59 days	4,932,340	289	encrypted HTTP, port 80	96	set of static IPs
Rustock	164 days	7,174,084	33	encrypted HTTP, port 80	1	static IP (208.72.169.54)
MegaD	113 days	198,799,848	1638	encrypted custom protocol, ports 80 and 443	21	static DNS name (majzufaiuq.info)
Srizbi	51 days	86,003,889	1848	unencrypted HTTP, port 4099	20	set of static IPs
Storm	50 days	961,086	20	compressed TCP	N/A	p2p (Overnet)

Table 1: **The botnets monitored in Botlab.** Table gives characteristics of representative bots participating in the seven botnets. Some bots use all available bandwidth to send more than a thousand messages per minute, while others are rate-limited. Most botnets use HTTP for C&C communication. Some do not ever change the C&C server address yet stay functional for a long time.



tions. All five anti-virus tools had signatures for only 192 of the 500 binaries, and we used only these 192 binaries in our validation. We considered a pair of binaries to be

to detect duplicates. Also, we observed a false-positive rate of 0.62%, where the anti-virus tags did not match, but network fingerprinting labeled the files as duplicates.

Our content clustering is performed by fetching the Web page content of all links seen in our incoming spam. We found that nearly 80% of spam pointed to just 11 distinct Web pages, and the content of these pages did not change during our study. We conclude that while spam-

to obtain their approximate spam list sizes. We present the size estimates at a confidence level of 95%. We estimate MegaD's spam list size to be *850 million addresses* ($\pm 0.2\%$), Rustock's to be *1.2 billion* ($\pm 3\%$), Kraken's to be *350 million* ($\pm 0.3\%$), and Storm's *110 million* ($\pm 6\%$).

We derive p using the number of spam messages received by our spam monitor and an estimate of the global number of spam messages. With our current setup, the former is approximately 2.4 million daily messages, while various sources estimate the latter at 100-120 billion messages (we use 110 billion) [14, 21, 32]. This

We analyze 46 million spam messages obtained from a 50-day trace of spam from University of Washington and

	Kraken	MegaD	Pushdo	Rustock	Srizbi	Storm
Canadian Healthcare	0%	0%	0.01%	22%	3%	0%
Canadian Pharmacy	16%	28%	10%	0%	9%	6%
Diamond Watches	22%	0.1%	0%	0%	13%	0%
Downloadable Software	0%	0%	25%	0%	0%	0%
Freedom From Debt Forever!	19%	0%	0%	0%	0%	1%
Golden Gate Casino	0%	32%	0%	0%	0%	0%
KING REPLICA	0%	4%	3%	0%	15%	0%
LNHSolutions	0%	6%	0%	0%	0%	0%
MaxGain+ ... No.1 for PE	0%	0%	3%	78%	0%	0%
Prestige Replicas	7%	0%	0.3%	0%	31%	0%
VPXL - PE Made Easy	20%	8%	6%	0%	24%	55%
Unavailable	3%	22%	38%	0%	0%	24%
Other	13%	0.1%	15%	0%	5%	14%