```
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.
```

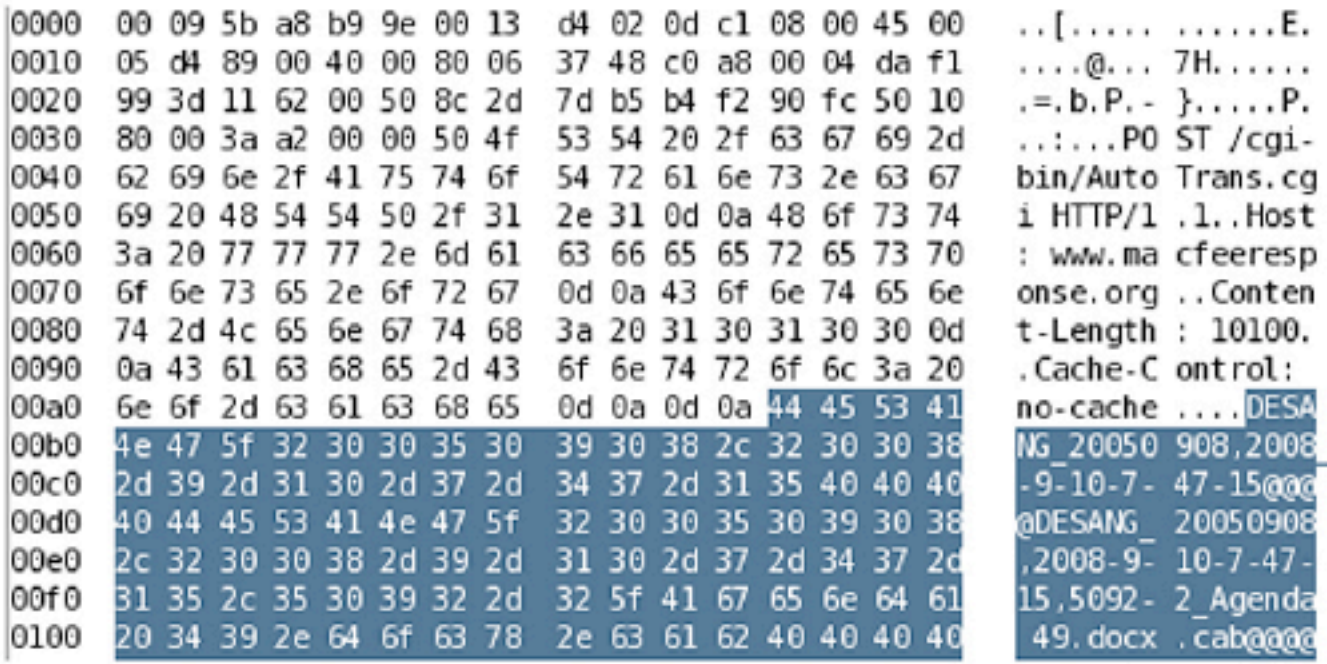
```
.visit              - flood URL with GET requests
.scan                    - scans a random range for vulnerable routers/modems
.rscan            - scans a CIDR range for vulnerable routers/modems
.lscan                   - scans the local subnet for vulnerable routers/modems
.lrscan                  - 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.

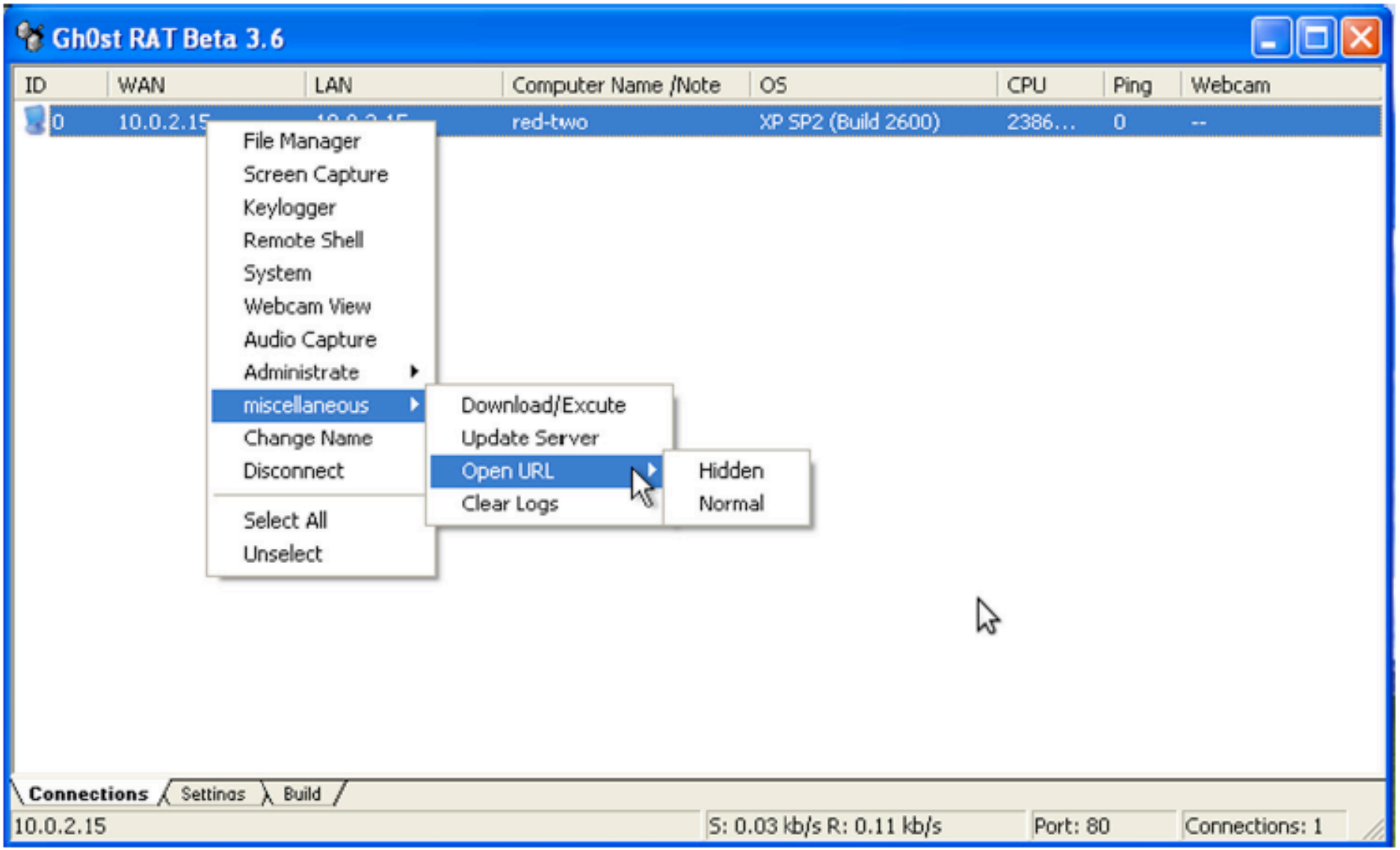
Introduction:

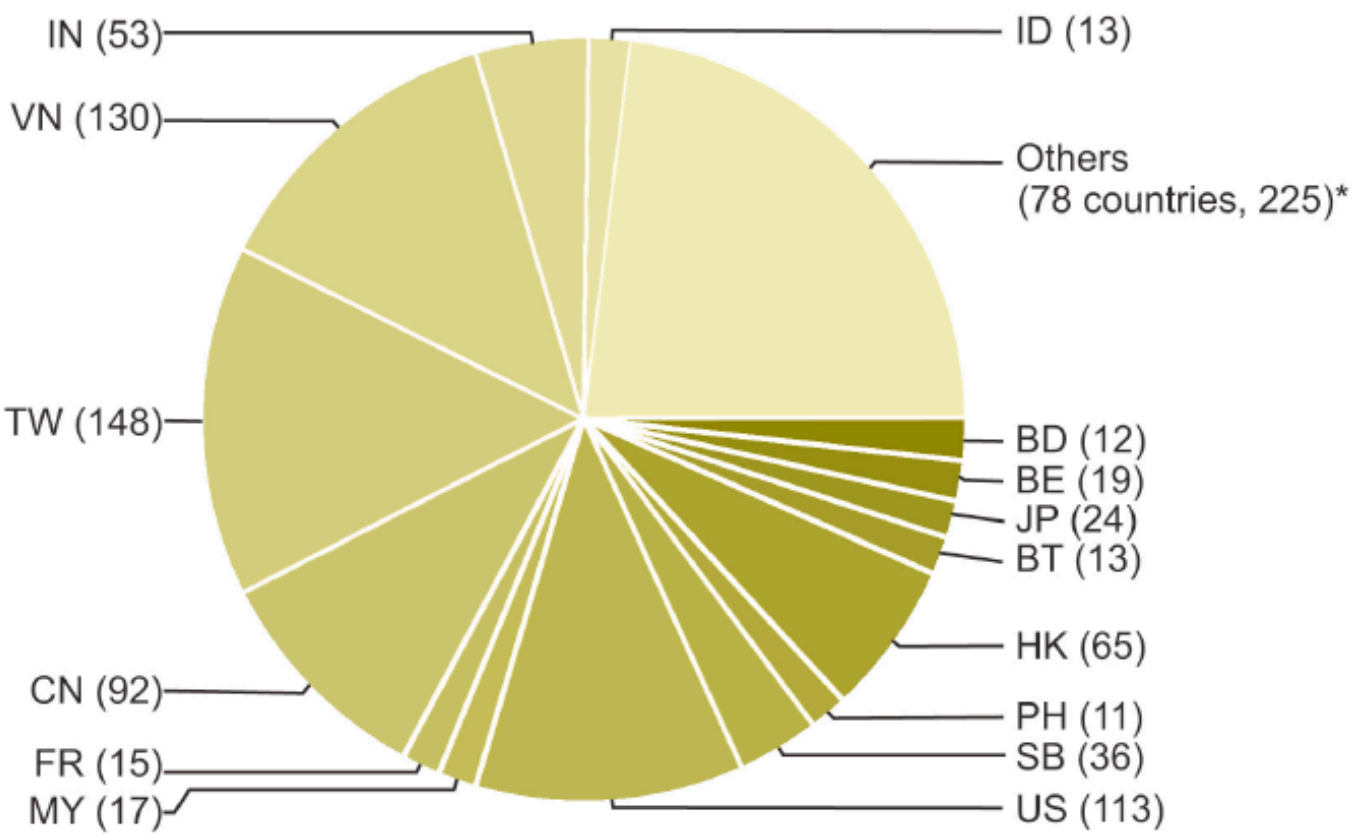
The NB5 was a popular ADSL/ADSL2+ modem-router, produced by Netcomm circa 2005. The NB5 is based on the Texas Instruments TNETD7300, featuring a 32bit RISC MIPS 4KEc V4.8 processor, 2MB of flash ROM, 8MB of RAM, Ethernet + USB connectivity, and runs an embedded Linux distribution.



```
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

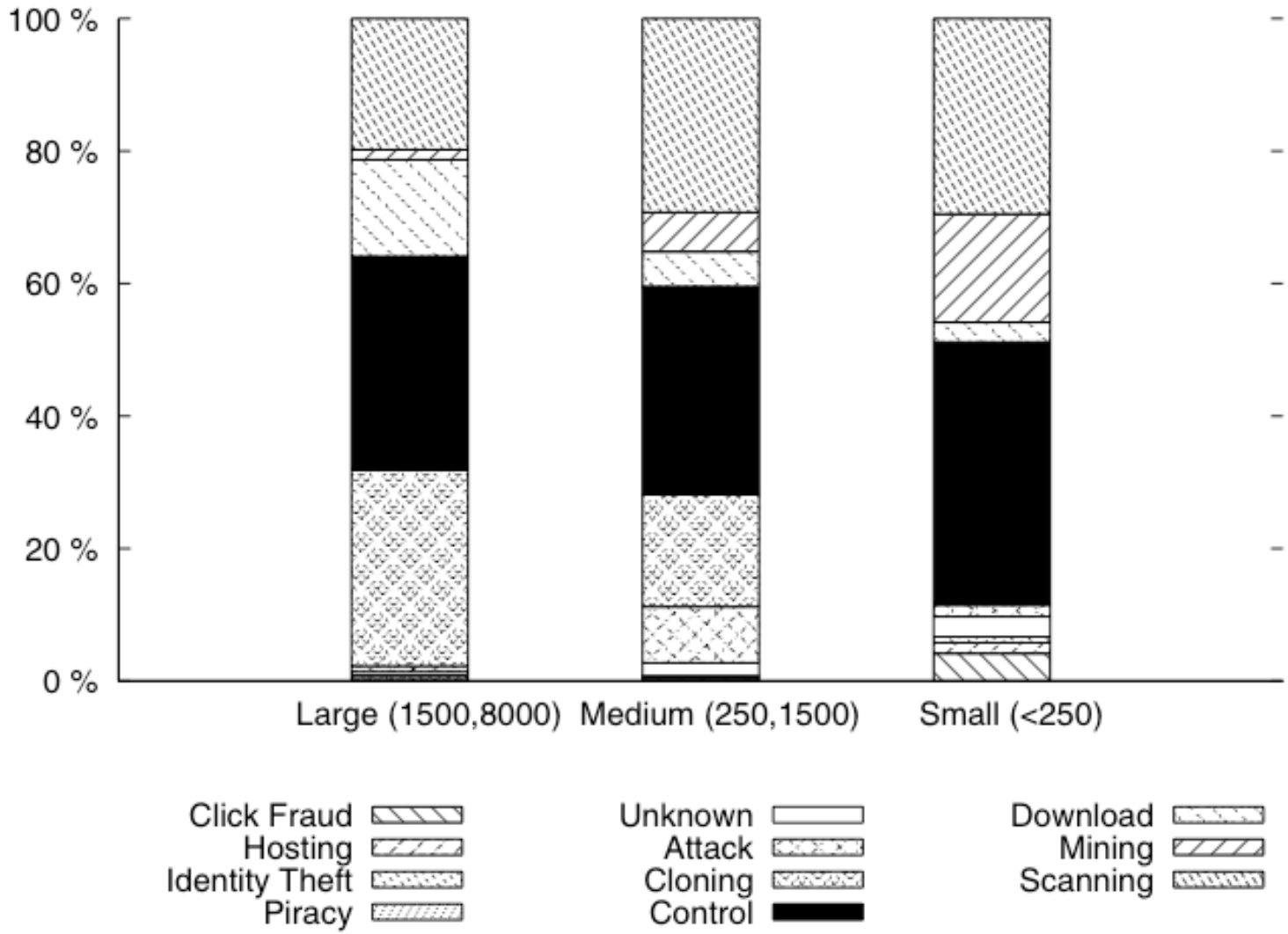
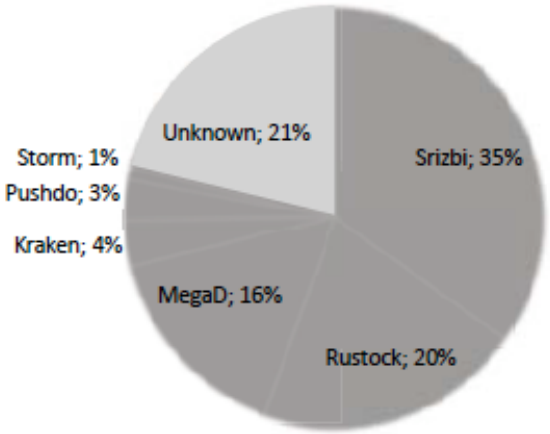
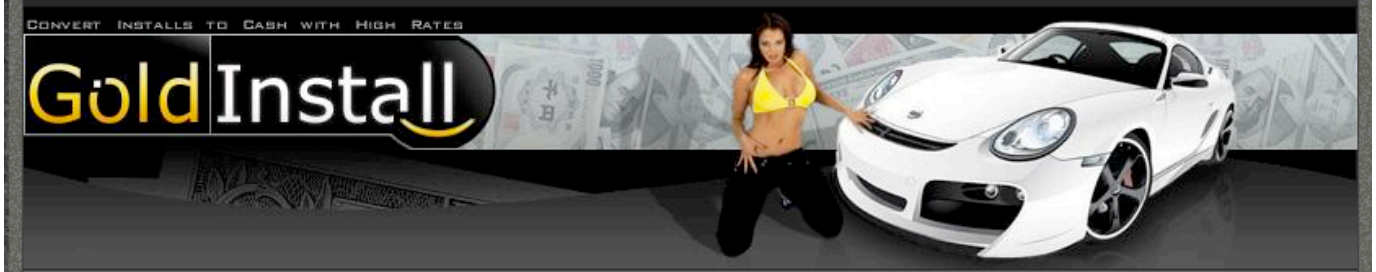


Figure 13: Percentage of command types as a function of observed botnet size.

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

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.



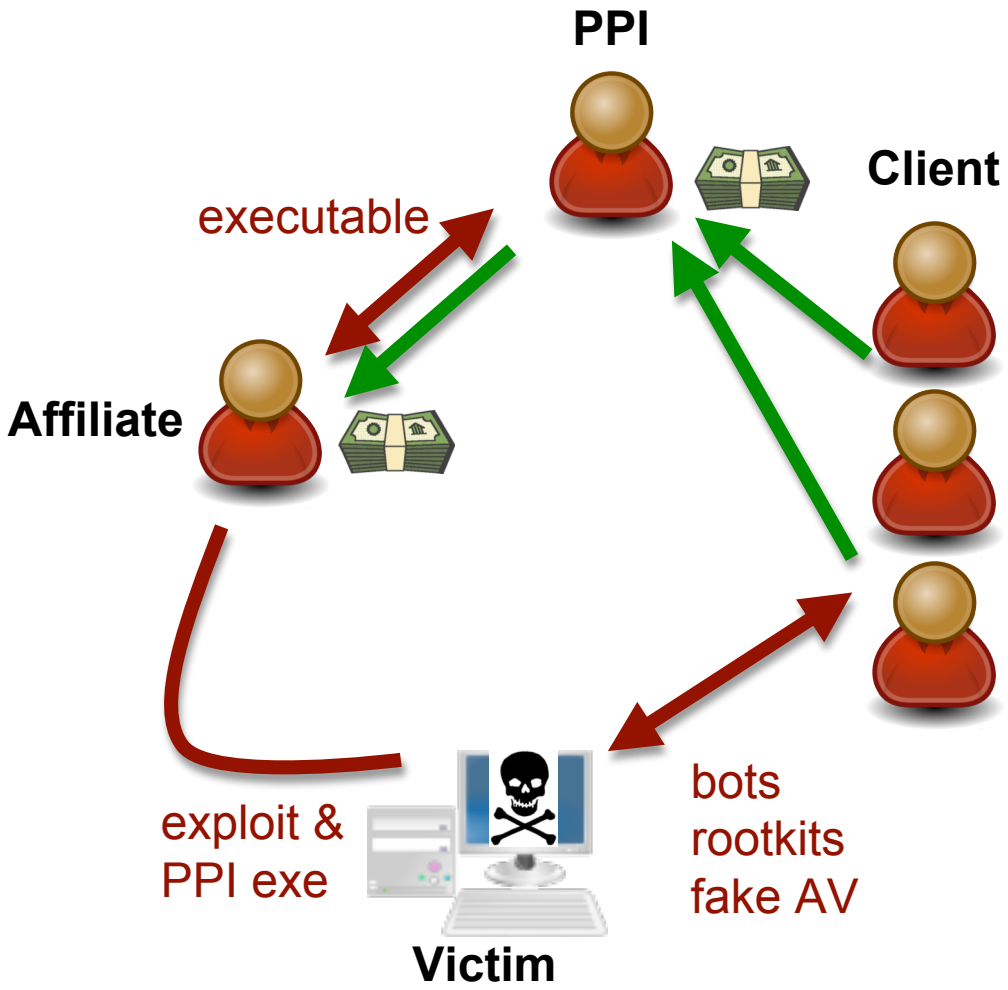


Main | Sign up | Login | Rates | Contacts | **Terms of service** | FAQ

Prices

Goldinstall Rates for 1K Installs for each Country.

Country	Price
OTH	13$
US	150$
GB	110$
CA	110$
DE	30$
BE	20$
IT	65$
CH	20$
CZ	20$
DK	20$
ES	30$
AU	55$
FR	30$
NL	20$
NO	20$
PT	30$
LB	6$


PPI
Client
executable
Affiliate
exploit &
PPI exe
bots
rootkits
fake AV
Victim

The life of a dropped executable

Over 12 binaries downloaded

Total Time: <5 minutes

Best Pay-Per-Install affiliate program reviews. ActiveX affiliates. - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://www.pay-per-install.com/ Go Links

PAY PER INSTALL AFFILIATE PROGRAMS

Today is: Tuesday 16. November 2010

CLICK HERE TO VISIT OUR BEST SPONSOR.

WE WORK
Even when you sleep!

One of the best PPI programs. Up to $180 per 1000 Installs.

Affiliate Program NewsLetter Get new programs via email

Insert your Email Address: Subscribe

JOIN MAKE MONEY FORUM

Learn How to make money with PPN Gateway

Free guide to teach you how to make $7000 per day

Best Pay-Per-Install affiliate program reviews. ActiveX affiliates.

BOOKMARK US

MAKE MONEY CATEGORIES
- Pay Per Click
- Pay Per Impression
- Bid Search Engines
- Pay Per Lead
- Pay Per Install

OTHERS
- CONTACT

GET PAID from each toolbar install

Best Pay-per-install affiliate programs on the net. Earn money with any traffic, these ActiveX affiliates will convert anything and make you rich. Payments are up to $1.50 per install. You usualy distribute installation of toolbar and making cash. You can also make loads of money with content sites such are movies, games, mp3 and protect your content with Content Gateways which are paying most, to unlock the content user needs to install simple adware application and than he can get content for free.

All Pages: [0] [1] [2] [3] [4]

Make money with these BEST AFFILIATE PROGRAMS

Rank Sponsors

BOOKMARK US

Last 10 Reviews
- CPALead - November/13/2010
- SexSearch - October/31/2010
- LoudMo - October/28/2010
- SexSearch - October/18/2010
- SexSearch - October/18/2010
- ioXes - October/12/2010
- Earning4u - September/09/2010
- Earning4u - August/30/2010

Make money with these BEST AFFILIATE PROGRAMS

Rank | Sponsors

Pinball Publisher Network

★★★★★

1

Pinball Publisher Network acquired assets from former ZangoCash - accounts are transferred so you can login same way as with ZangoCash.

Pinball Publisher Network - PPN is now highest quality Pay Per Install business model company on the Internet these days. They are much more strict so no fraud webmasters get into their system. They also have to follow laws so they will stay on the market long time.
PPN pays much more than other pay per install affiliate programs. PPN will pay you from $0.75 to $1.45 per USA, Canada and UK installation, $0.40 to $0.75 for France, Germany, Netherlands installs and $0.10 to $0.24 for these countries Australia, Austria, Belgium, Denmark, Finland, Ireland, Mexico, New Zealand, Norway, Portugal, Sweden, Switzerland installations. So you get paid every time someone installs from those countries. Also the ranges are moved so you get better rates for less installs.
PPN has great referral program with incredible rate of 20% so you will make 20% of your downline earnings forever.
There is many ways how to promote Pinball Publisher Network such as Syndication, DRM, Media Restrictor, Toolbar Download and others. You get always paid by paypal, check or wire transfer.

There are strict rules set by PPN and one of them is that you must have top level domain name like www.domainname.com. If you do not have than do not bother to signup with them because this shows how immature webmaster you are and you would not be accepted by PPN staff.
Traffic is also recommended (no traffic, no money) :)

Rating 3 | Votes 11 | Hits 3730 | 13 th Aug 2009

Recommend it!

Your comments (2) WRITE/READ

Category: | **Pay Per Install** | **Pay Per Impression** | **Pay Per Click** |

Earning4u

★★★★

LoudMo

★★★★★

LoudMo is an awesome new PPI pay per install affiliate program that stands out from the competition with high payouts at $1.50 per install, great conversions, and the latest gateways and tools to make you money.

The tier system for LoudMo isn't as confusing as the other PPI programs like Zangocash, PinballNetwork and Vombacash. You get paid $1.50 for US installs, $0.60-$0.15 for the other big countries and the best news is that you still get paid for installs from ANYWHERE in the world. Not like the other PPI programs that only pay for limited countries.

There's also a great affiliate referral program that's really good for earning extra cash. If you start referring new affiliates to LoudMo, you earn a 5% revshare. That means that if a new affiliate signs up using your referral link, you get 5% of their future revenue EVERY MONTH. So, if you get a friend to sign up and they get 6000 installs a month, you earn around $5,000 in only 3 months.

The products for LoudMo are also really cool. Gateway content protection technology lets you provide free content and make money, the free FLV direct player allows users to save and play flash videos from tube sites, and the best one is Chameleon Tom which is going to be really popular. It lets people change their Facebook profile page to look different with images and stuff. All of these installation products make it really easy to earn tons of money, especially with the high rate of $1.50 per install.

Dont forget that you will need TOP LEVEL DOMAIN name before you register... webmasters without operating website are approved slowly.

Rating 7.8

Votes 5

Hits 2014

10 th Nov 2009

Recommend it!

Category: | **Pay Per Install** |

Your comments (10) WRITE/READ

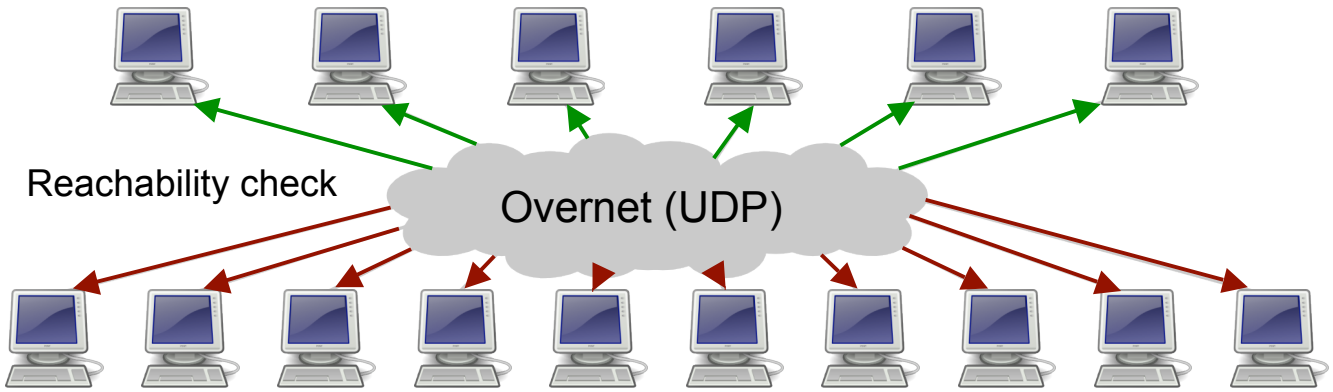
Welcome to Storm!

Would you like to be one of our newest bots?

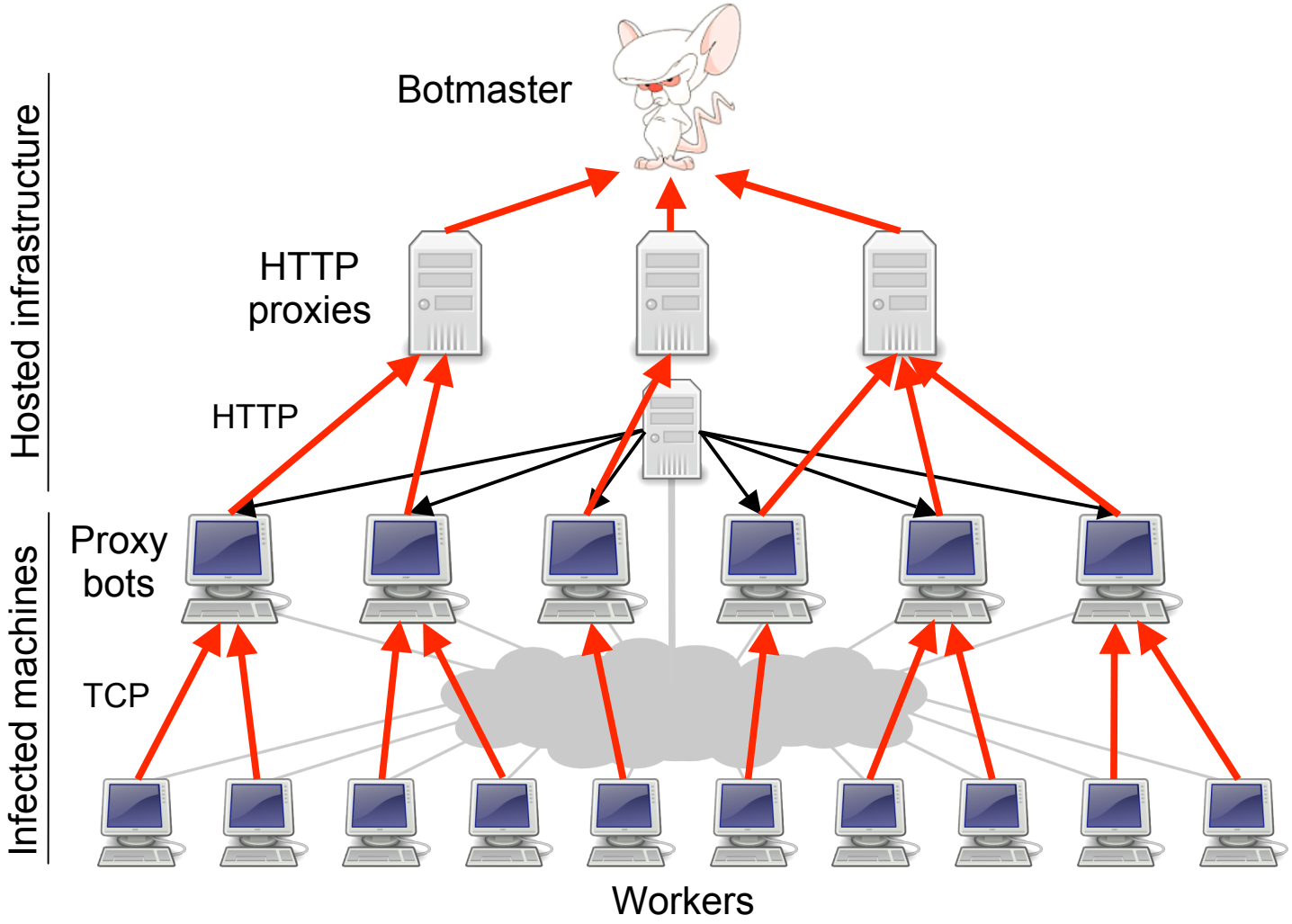
Just read your postcard!

(Or even easier: just wait 5 seconds!)

The Storm botnet



The Storm botnet



Google translate http://goohost.ru/ Translate

Translate from: Russian Translate into: English

Help | Sign in

View: Translation Original

GooHost.ru

Reliable and quality hosting

Тел.: +7(495) 542-39-87, icq: 418396204

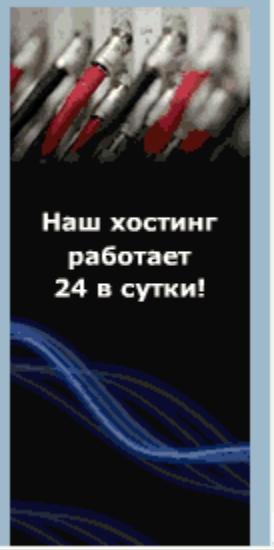
Menu

- Hosting Plans
- Email Mailing
- Website Design
- FAQ
- Dedicated server
- Domain Registration
- Payment
- Contact

Hosting Plans

We offer a complaint-resistant hosting to host your sites, which are specified in mass mailings.

We decided to bring visitors to your web site through unsolicited mass emails? Wonderful idea! You certainly expect a boom visits. But! As in any ointment and then not pass without a spoon of tar ... Alas, but your wonderful site, shortly after the start of spam mail, will be closed due to flood of complaints from postal services. Is there a way to avoid these problems? Of course! Our complaint-resistant hosting simply ignores any complaints, all postal services, and you can be rest assured about the performance of their sites - they will not be closed. And you get new customers, expand their business and increase their sales and revenue, thanks to spam mailing lists.



Internet

Obuzoustoychivy hosting is more expensive than usual, but you will have the full guarantee that your site no one ever closes, it will always be available to your customers!

MINI PLAN	
Volume disc	400 MB
Domains	1
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	4 000 rub. / 1 month.

STARTER PLAN	
Volume disc	500 mb
Domains	3
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	5 000 rub. / 1 month.
BUSINESS PLAN	
Volume disc	1000 mb
Domains	7
Traffic *	Unlimited
FTP-access	there is
MySQL database	there is
Control panel	there is
COST	7 000 rub. / 1 month.
PREMIUM PLAN	

Security Fix

Brian Krebs on Computer Security

SEARCH THIS BLOG

Go

RECENT POSTS

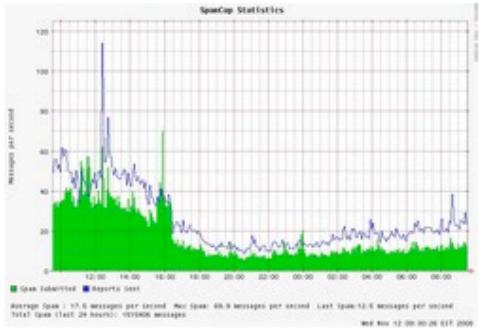
- E-Banking on a Locked Down PC, Part II
- ChoicePoint Breach Exposed 13,750 Consumer Records
- President Obama on Cyber Security Awareness
- Mozilla Disables Microsoft's Insecure Firefox Add-on
- PayChoice Suffers Another Data Breach

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-

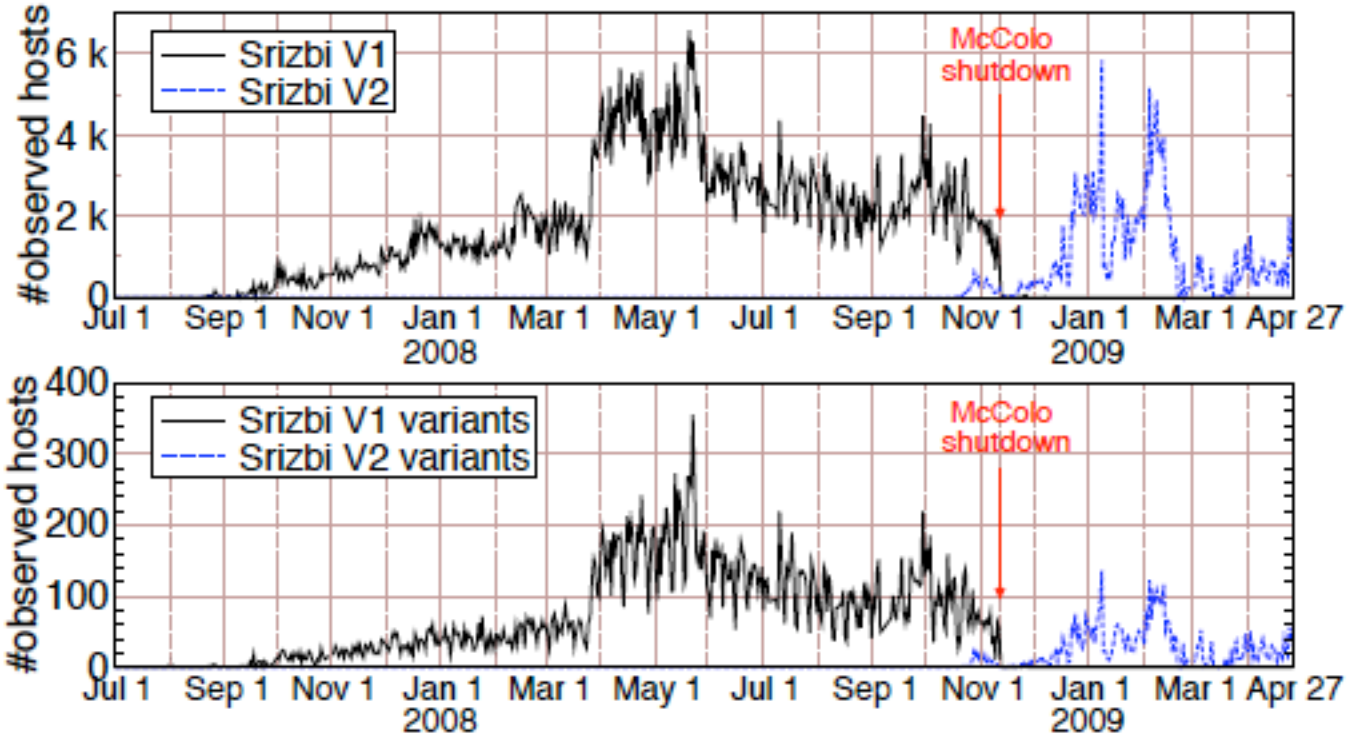


Figure 3: Number of observed hosts infected with Srizbi V1/V2 (top) and their variants (bottom) in the MAWI data set.

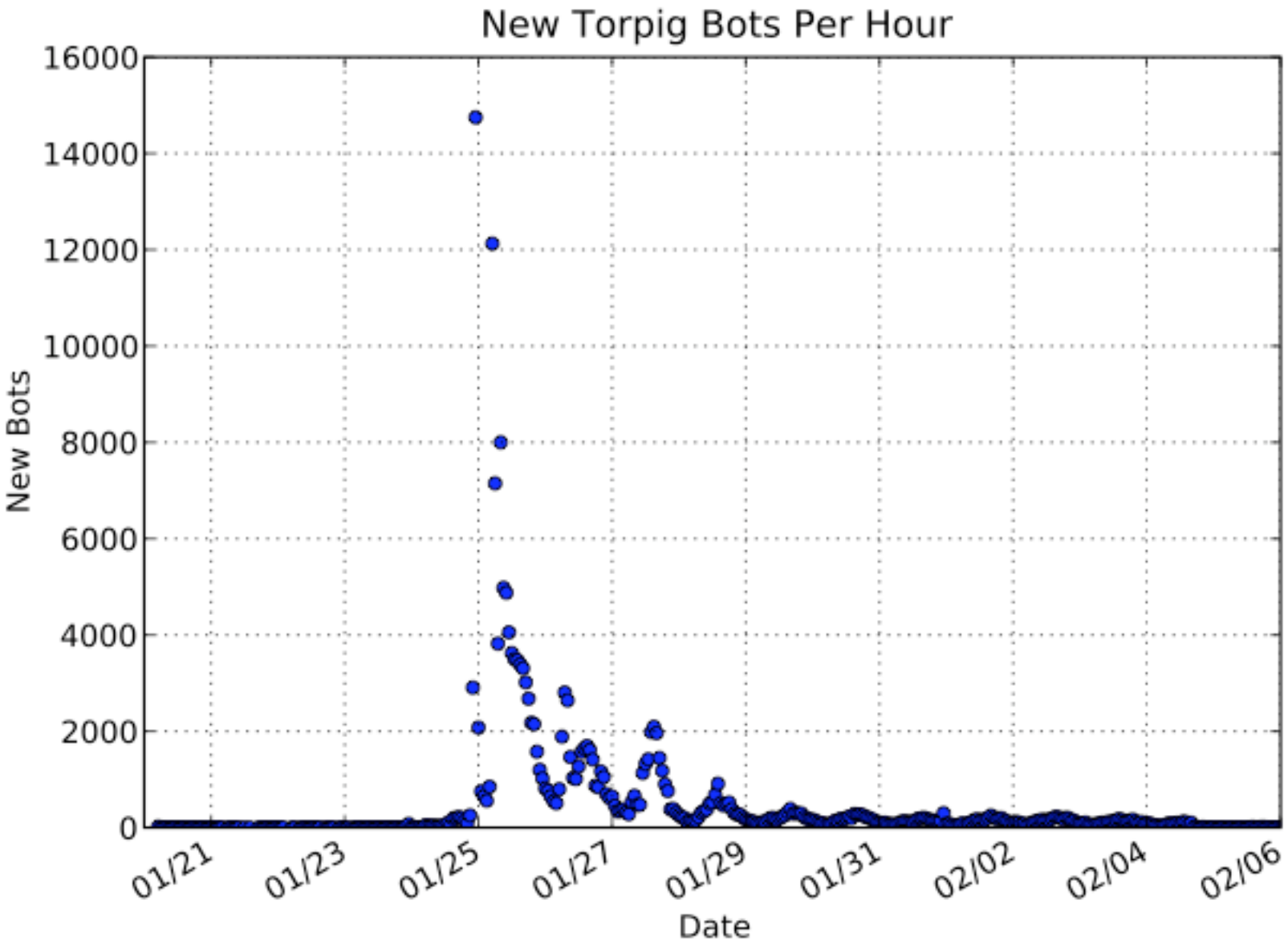


Figure 6: New bots per hour.

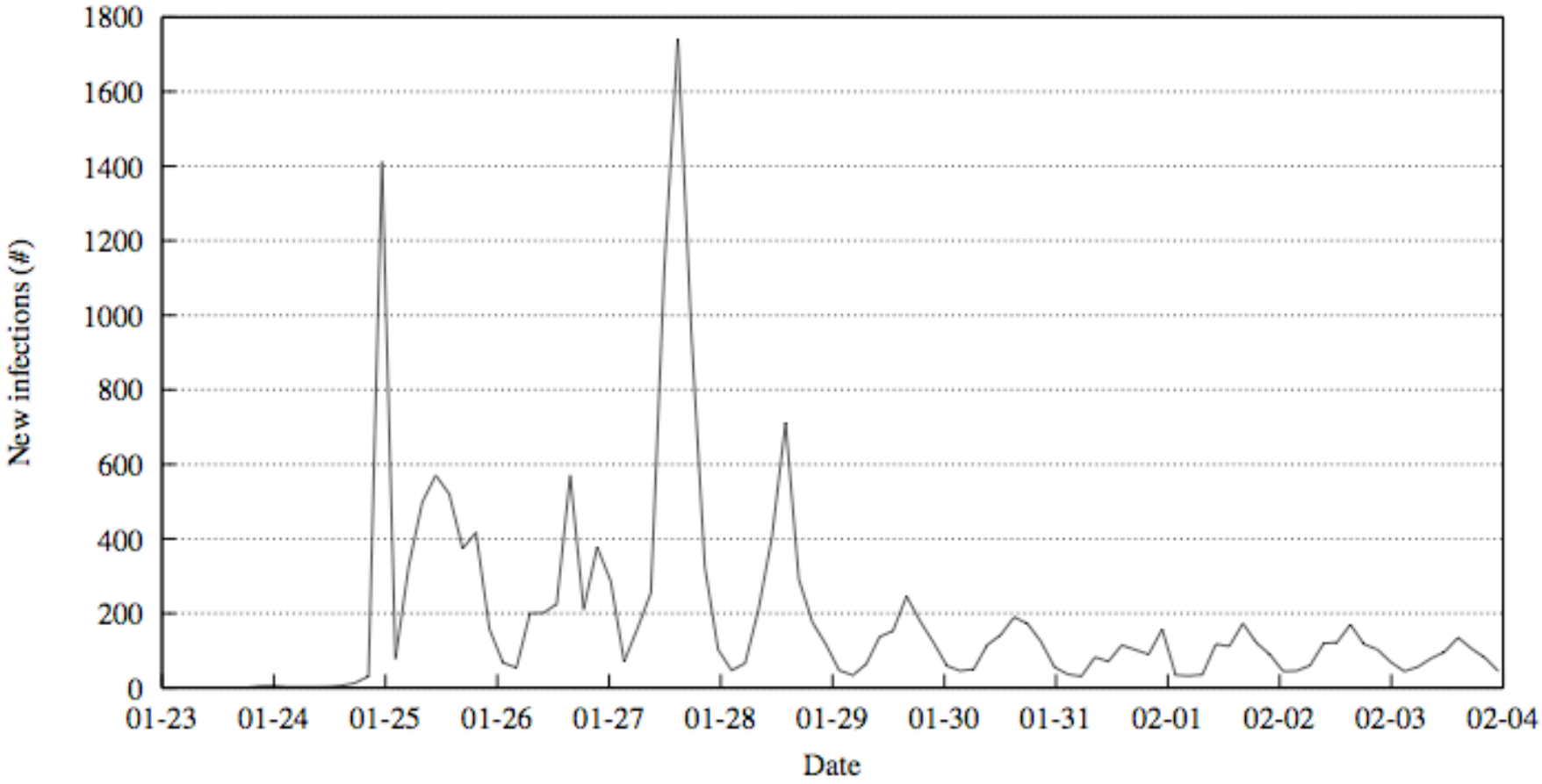


Figure 11: New infections over time.

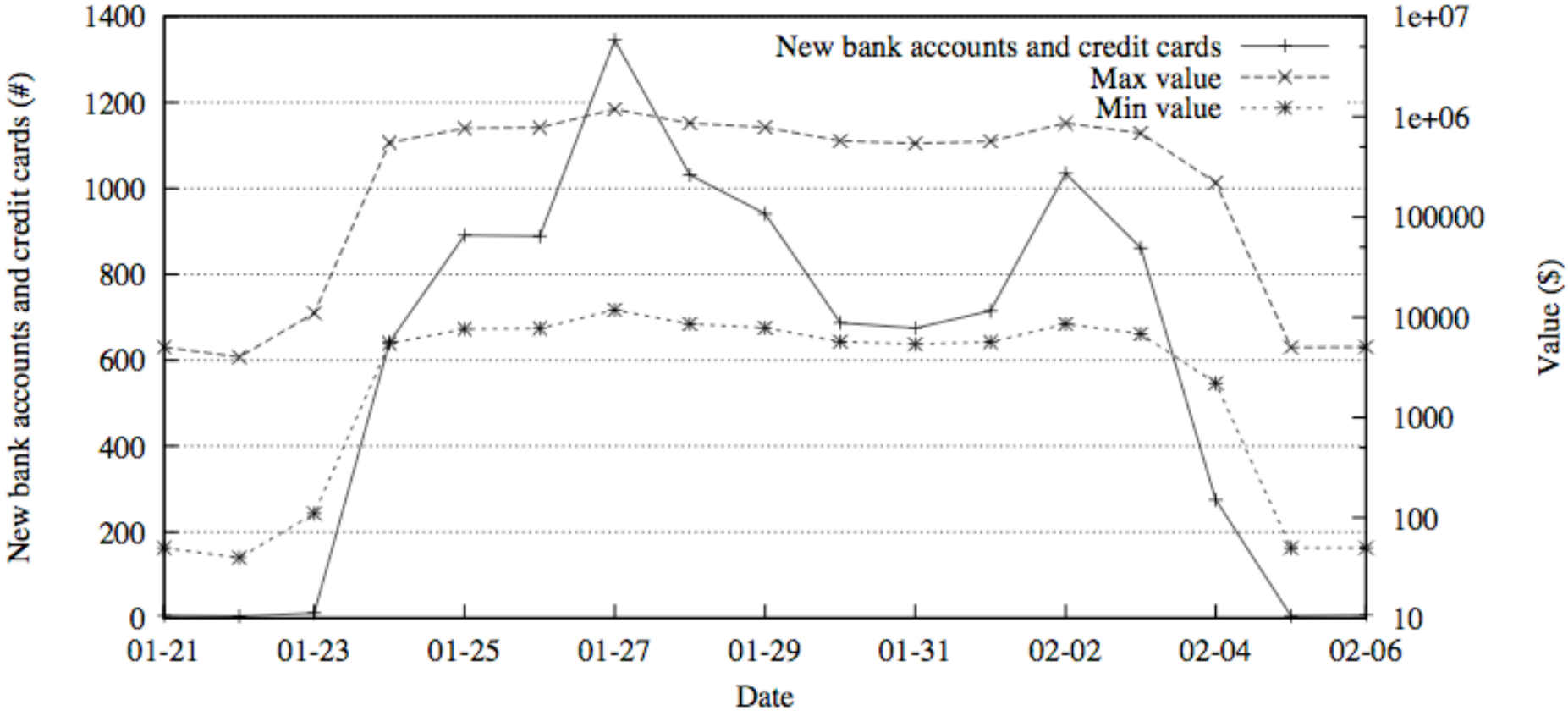


Figure 12: The arrival rate of financial data.