

## The Spam Problem

Suresh Ramasubramanian, IBM

Joe St Sauver, M<sup>3</sup>AAWG Senior Technical Advisor

October 2012

New Delhi

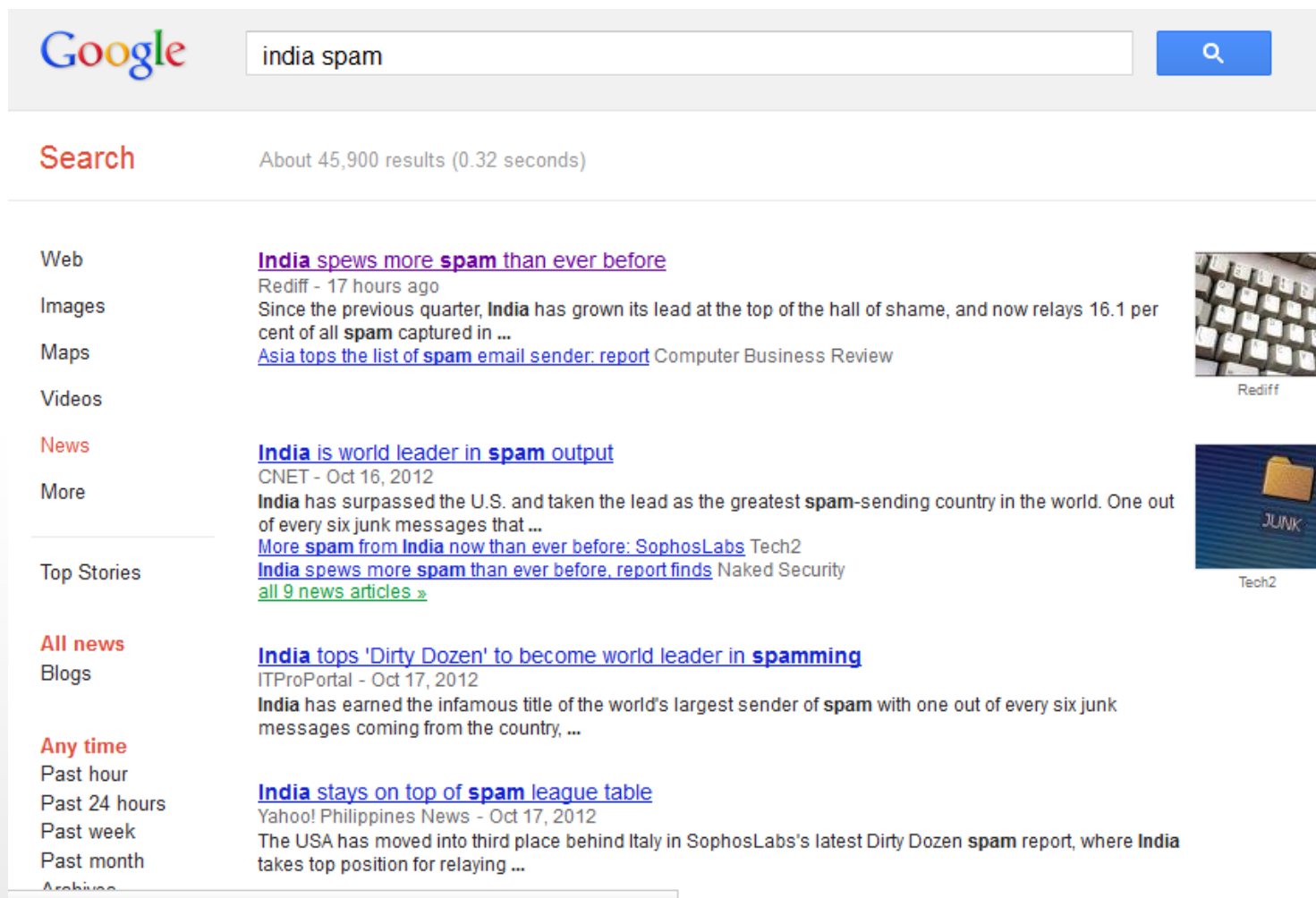


# India has a serious spam problem

please help us help you to tackle it

Suresh Ramasubramanian  
Joe St Sauver

# We have all seen headlines like this:



Google search for "india spam" showing results. The search bar contains "india spam" and the search button is visible. The results page shows "Search" with "About 45,900 results (0.32 seconds)".

**Web**  
[India spews more spam than ever before](#)  
Rediff - 17 hours ago  
Since the previous quarter, **India** has grown its lead at the top of the hall of shame, and now relays 16.1 per cent of all **spam** captured in ...  
[Asia tops the list of spam email sender: report](#) Computer Business Review

**Images**

**Maps**

**Videos**

**News**  
[India is world leader in spam output](#)  
CNET - Oct 16, 2012  
**India** has surpassed the U.S. and taken the lead as the greatest **spam**-sending country in the world. One out of every six junk messages that ...  
[More spam from India now than ever before: SophosLabs](#) Tech2  
[India spews more spam than ever before, report finds](#) Naked Security  
[all 9 news articles »](#)


**More**

**Top Stories**


**All news**  
**Blogs**  
[India tops 'Dirty Dozen' to become world leader in spamming](#)  
ITProPortal - Oct 17, 2012  
**India** has earned the infamous title of the world's largest sender of **spam** with one out of every six junk messages coming from the country, ...

**Any time**  
Past hour  
Past 24 hours  
Past week  
Past month  
Archive

[India stays on top of spam league table](#)  
Yahoo! Philippines News - Oct 17, 2012  
The USA has moved into third place behind Italy in SophosLabs's latest Dirty Dozen **spam** report, where **India** takes top position for relaying ...



Rediff



Tech2

# Offers like this keep landing in our inboxes

## Email Database India

### Email Database India Offer

#### 10 database+ products at just Rs. 1500/- (USD 35)

4K Indian email id (general)

75K Indian business people database

27 lacs Indian email ids (city wise) ( for 12 major Indian cities)

50K Mumbai email database

1 million worldwide email database

1.5 lacs NRI database

10k MCA students email database

25 Crore Great Worldwide Email Database (free)

4 Million MSN

6 Million AOL

14 Million Hotmail

1 Million Compuserve

297 Million other

+ EMAILING SOFTWARE

+ Free readymade brochure / leaflet for sending through email

ALL THE ABOVE MENTIONED PRODUCTS AT JUST Rs. 1500/- (USD 35)


---

No need to spend thousands of Rupees to buy email database India. We have bought it at a higher price from the original vendors. Now, we are re-selling at a much cheaper price.



Just send Us Rs. 1000/- (USD 25) and we will send you the link to download the database.

# Which, unsurprisingly, leads to spam like this: [I don't live in Jaipur, by the way]

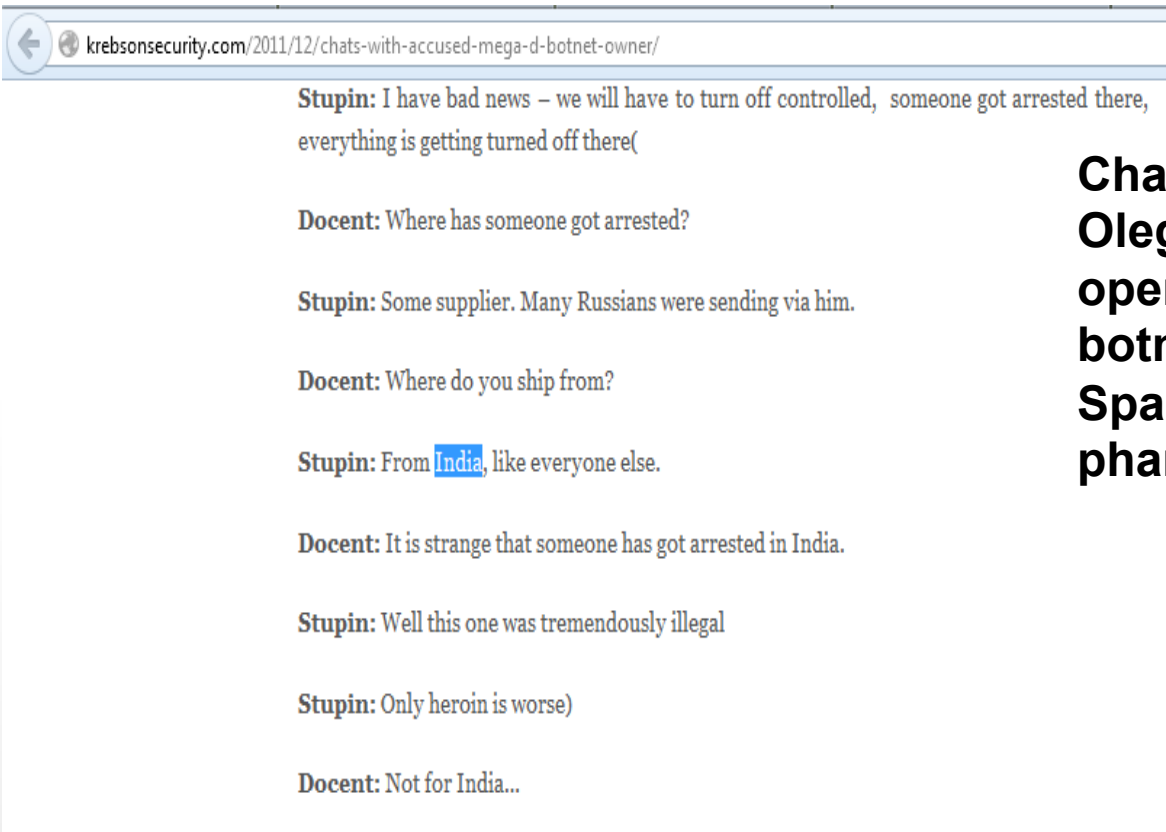
An excellent opportunity to book your own dream plot in just Rs. 13500/-

 Smart Meadows & Shree City [Schedule cleanup](#) 10/19/12 | [Groups](#)  
To: sramasubramanian@hotmail.com ▾

[Click here to view it in a Web Browser](#)

 <p><b>A Smart 125 Acre Township</b> Jaipur-Ajmer Expressway NH-8</p> <p><b>Price Rs. 1800/Sq.Yds</b></p>	 <p><b>150 Acre of Integrated Township</b> Tonk Road NH-12, Chaksu Jaipur</p> <table border="1"><tbody><tr><td><b>Plot Price:</b> Rs.1350/Sq.Yd</td><td><b>Farmhouse Price:</b> Rs.900/Sq.Yd</td></tr></tbody></table>	<b>Plot Price:</b> Rs.1350/Sq.Yd	<b>Farmhouse Price:</b> Rs.900/Sq.Yd
<b>Plot Price:</b> Rs.1350/Sq.Yd	<b>Farmhouse Price:</b> Rs.900/Sq.Yd		

# India is a major part of the “supply chain” for pharmacy spam



**Chat between two Russians— Oleg Nikolayenko (Docent), operator of the Mega-D botnet, and Dmitri Stupin of SpamIt, a major illegal online pharmacy operation**

*Courtesy Brian Krebs – [www.krebsonsecurity.com](http://www.krebsonsecurity.com)*

# Some scams are uniquely Indian, like this bunch of fake call centers mostly based in Kolkata:

## FTC cracks down on tech support scam run from India

Phone con attempted to convince people that their computers had a virus and then sign them up to multi-year contracts

---

**Charles Arthur**

[guardian.co.uk](http://guardian.co.uk), Thursday 4 October 2012 11.06 BST

# And let us not forget the good old Nigerian scam – now customized for India

From: Radha Ramalinga <[radharamalinga2@gmail.com](mailto:radharamalinga2@gmail.com)>  
Date: 2011/2/14  
Subject: Namaste  
To:

Namaskar,

My name is Radha Ramalinga, I am the wife of B. Suryanarayana Raju Ramalinga, the younger brother of Byrraju Ramalinga Raju, former chairman, founder and owner of Satyam Computers.

I do have a proposal for you, which would be of immense financial benefits to you and I.

You are here: HOME > MUMBAI > Report

## Nigerian lottery scam: Police looking for Indian accomplices

Published: Saturday, Jun 2, 2012, 18:16 IST  
Place: Thane | Agency: PTI



# A huge spam problem means a very large number of Indian IPs get blocked in various spam block lists



Found 35 SBL listings for IPs under the responsibility of

SBL141615	122.165.85.169/32
05-Jun-2012 16:49 GMT	ZeuS botnet controller @122.165.85.
SBL138215	182.72.113.24/29
06-May-2012 05:15 GMT	indian spammer - optimosys
SBL107898	122.184.133.210/32
17-Apr-2011 13:48 GMT	Forum/Comment spam source @122.

Data from the Spamhaus Project <http://www.spamhaus.org>

# The number of IPs blocked for virus traffic is huge

Extensive broadband penetration + insecure PCs = trouble

ASN	Listings	%total	% Total Listings	%cumulative Total Listings	Rank	Traffic	%Traffic	Spams/Bot	Size(K)	Infect %
Total	8590666	100				214441085	100	24.96		
<a href="#">AS9829 sancharnet.in IN</a>	579129	6.74	6.74	6.74	1	1636977	0.76	2	4944.2	11.439%
<a href="#">AS45899 vnnic.net.vn VN</a>	367659	4.28	4.28	11.02	2	390763	0.18	1	2364.8	15.183%
<a href="#">AS9121 telekom.gov.tr TR</a>	350752	4.08	4.08	15.10	3	84450	0.04	0	12433.5	2.755%
<a href="#">AS45595 ptcl.net.pk PK</a>	338669	3.94	3.94	19.05	4	145875	0.07	0	5446.2	6.073%
<a href="#">AS4134 chinanet.cn.net CN</a>	317714	3.70	3.70	22.74	5	319787	0.15	1	110731.8	0.280%
<a href="#">AS6147 unired.net.pe PE</a>	165644	1.93	1.93	24.67	6	1739929	0.81	10	2643.8	6.119%
<a href="#">AS24560 airtel.in IN</a>	161209	1.88	1.88	26.55	7	238983	0.11	1	2490.0	6.323%
<a href="#">AS25019 saudi.net.sa SA</a>	154768	1.80	1.80	28.35	8	215178	0.10	1	3197.8	4.726%
<a href="#">AS17803 powersurfer.net IN</a>	144849	1.69	1.69	30.04	9	153368	0.07	1	1491.2	9.486%
<a href="#">AS7552 vnnic.net.vn VN</a>	133071	1.55	1.55	31.59	10	141399	0.07	1	9946.0	1.307%

Data from the Spamhaus CBL Project – <http://cbl.abuseat.org>

# The .in ccTLD too has spam problems

www.symantec.com/connect/blogs/rise-urls-spam

## Rise of .in URLs in Spam

Updated: 15 May 2012 | Translations available: 日本語

Eric Park SYMANTEC EMPLOYEE

+1  
1 Vote

Symantec. Official Blog

Share in Tweet Like

Symantec has observed an increase in spam messages containing URLs using the country code top-level domain (ccTLD) for India. This chart shows percentage of spam containing .in URLs:

Date	Percentage
5/14	0.1%
7/14	0.2%
9/14	0.3%
10/14	5.5%
11/14	0.5%
1/14	1.5%
3/14	1.8%
5/14	3.5%
6/14	4.5%
7/14	2.0%



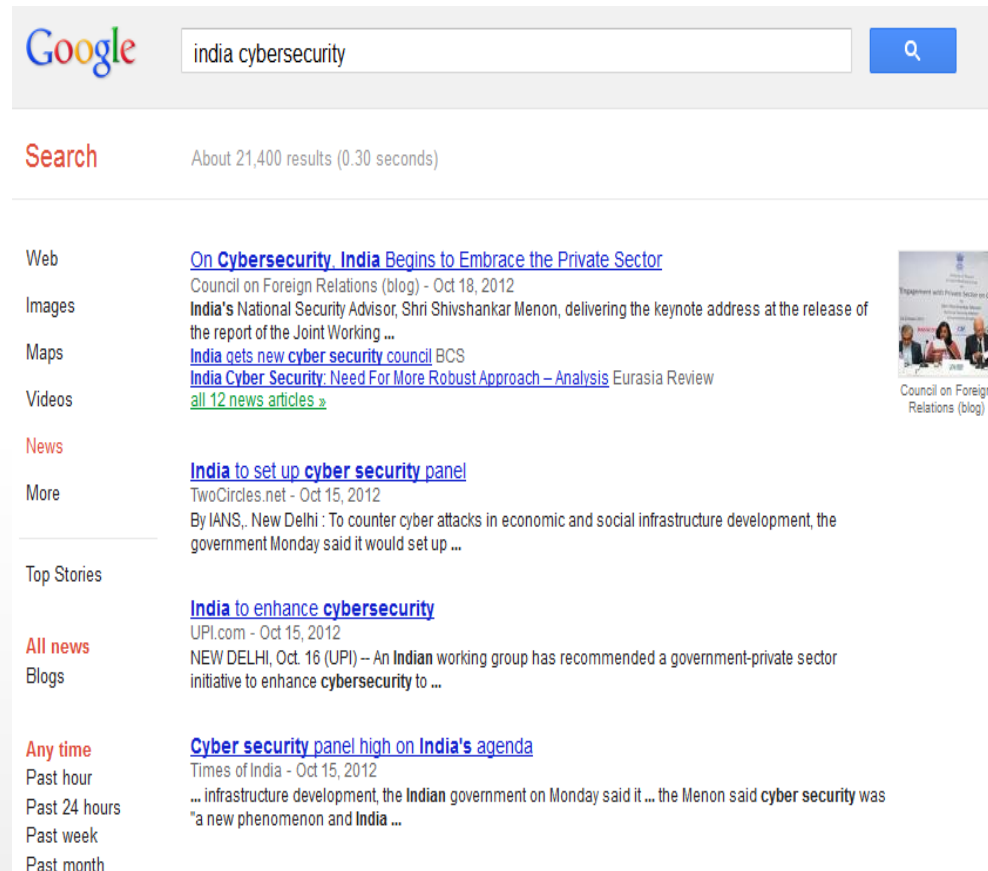
URI REPUTATION DATA

Homepage Lists Links News

325433	com
113261	ru
74304	info
58847	net
44816	in

*Courtesy Symantec and the SURBL Project*

# Fortunately, there are also headlines such as these . . .



Google

**Search** About 21,400 results (0.30 seconds)

**Web** [On Cybersecurity, India Begins to Embrace the Private Sector](#)  
Council on Foreign Relations (blog) - Oct 18, 2012

**Images** [India's National Security Advisor, Shri Shivshankar Menon, delivering the keynote address at the release of the report of the Joint Working ...](#)

**Maps** [India gets new cyber security council](#) BCS

**Videos** [India Cyber Security: Need For More Robust Approach – Analysis](#) Eurasia Review  
[all 12 news articles »](#)

**News** [India to set up cyber security panel](#)  
TwoCircles.net - Oct 15, 2012

**More** By IANS., New Delhi : To counter cyber attacks in economic and social infrastructure development, the government Monday said it would set up ...

**Top Stories** [India to enhance cybersecurity](#)  
UPI.com - Oct 15, 2012

**All news** [NEW DELHI, Oct. 16 \(UPI\) – An Indian working group has recommended a government-private sector initiative to enhance cybersecurity to ...](#)

**Blogs**


**Any time** [Cyber security panel high on India's agenda](#)  
Times of India - Oct 15, 2012

**Past hour** ... infrastructure development, the Indian government on Monday said it ... the Menon said cyber security was

**Past 24 hours** "a new phenomenon and India ...

**Past week**

**Past month**



# What can Indian ISPs do about messaging abuse?

## Spam and virus filter email and messaging (social, SMS...)

- Inbound / Outbound filtering, [Webmail filtering](#), [Port 25 management](#), [Sender Authentication](#), [Complaint Feedback Loops](#)

## Network security and threat mitigation

- Sinkholing botnet C&C IPs / domains, [Walled Garden](#) to isolate infected users
- [RFC 6561](#) – prepared with extensive contributions from M<sup>3</sup>AAWG members
- [M<sup>3</sup>AAWG Best Practices To Address Online and Mobile Threats](#)

## Abuse Desk Management

- Removing spammers from your network
- Vetting to ensure they don't become customers

# More things to do for ISPs

## User education and access to secure computing resources

- Discounted (or free?) antivirus included in DSL setup CDs
- DSL / Wi-Fi routers with non default passwords and firewalling
- Educate your customers about spam / scams / viruses

Join and interact with your peers around the world:

[M<sup>3</sup>AAWG](#), [APRICOT](#), [SANOG](#)

Local cooperation against spam and online threats

ISPAI working group, coordination with CERT-IN...

# How Indian email marketers can help

- Adopt the M<sup>3</sup>AAWG Sender Best Communications Practices
- Vet your new customers and audit existing customer lists
- Work to ensure your colleagues in the industry don't spam
- Adopt a shared code of conduct?
- Industry associations you can consider joining M<sup>3</sup>AAWG, ESPC, and of course, IAMA

# Government & Law Enforcement - Suggestions



Mitigation of malicious domains, botnet C&C etc.

- Data sharing by additional trusted third parties with CERT-IN

Stepped up action against local criminals

- Vendors of email address databases, unsolicited bulk email and SMS products and services, other parts of the cybercrime ecosystem (illegal drug suppliers, fake call centres.)

Increased engagement with intergovernmental and public/private groups

- [The Budapest Convention on Cybercrime](#)
- [The London Action Plan against Spam](#)
- [FIRST](#) / [APCERT](#), [M<sup>3</sup>AAWG](#), [OECD WPISP](#) ...



# Localization of M<sup>3</sup>AAWG best practice documents



Several best practice documents published by M<sup>3</sup>AAWG are currently available in Arabic, Spanish, Chinese and French, translated from the original English version.

We welcome volunteers to translate these documents into Hindi and other Indian languages. If you are interested in helping out, please feel free to email us.

# Thank You