The Spam Problem

Suresh Ramasubramanian, IBM
Joe St Sauver, M³AAWG Senior Technical Advisor
October 2012
New Delhi

M3AAWG
MESSAGING MALWARE MOBILE

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:

M3AAWG
MESSAGING MALWARE MOBILE

Google india spam

Search About 45,900 results (0.32 seconds)

Web
Images
Maps
Videos
News
More

Top Stories

All news
Blogs

Any time
Past hour
Past 24 hours
Past week
Past month

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


Rediff

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 »

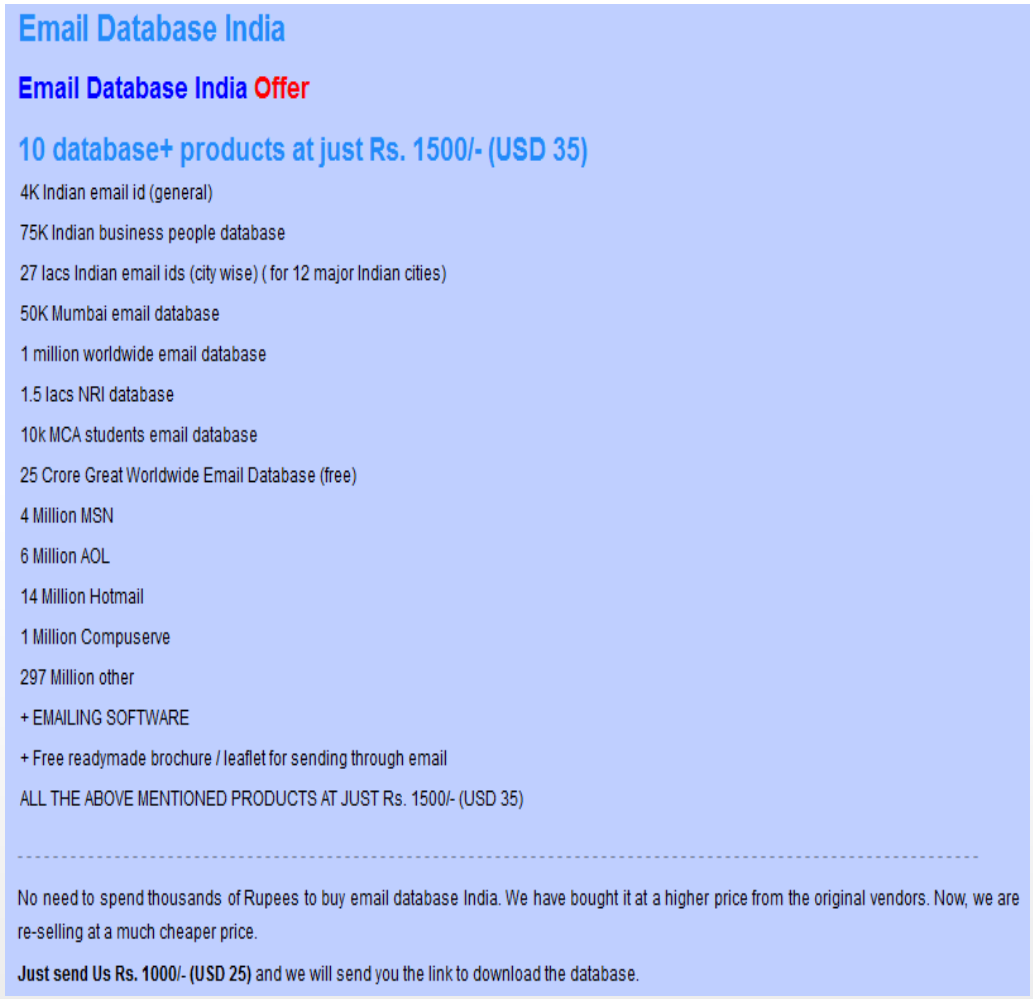
Tech2

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, ...

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 ...

Offers like this keep landing in our inboxes

M³AAWG
MESSAGING MALWARE MOBILE



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.

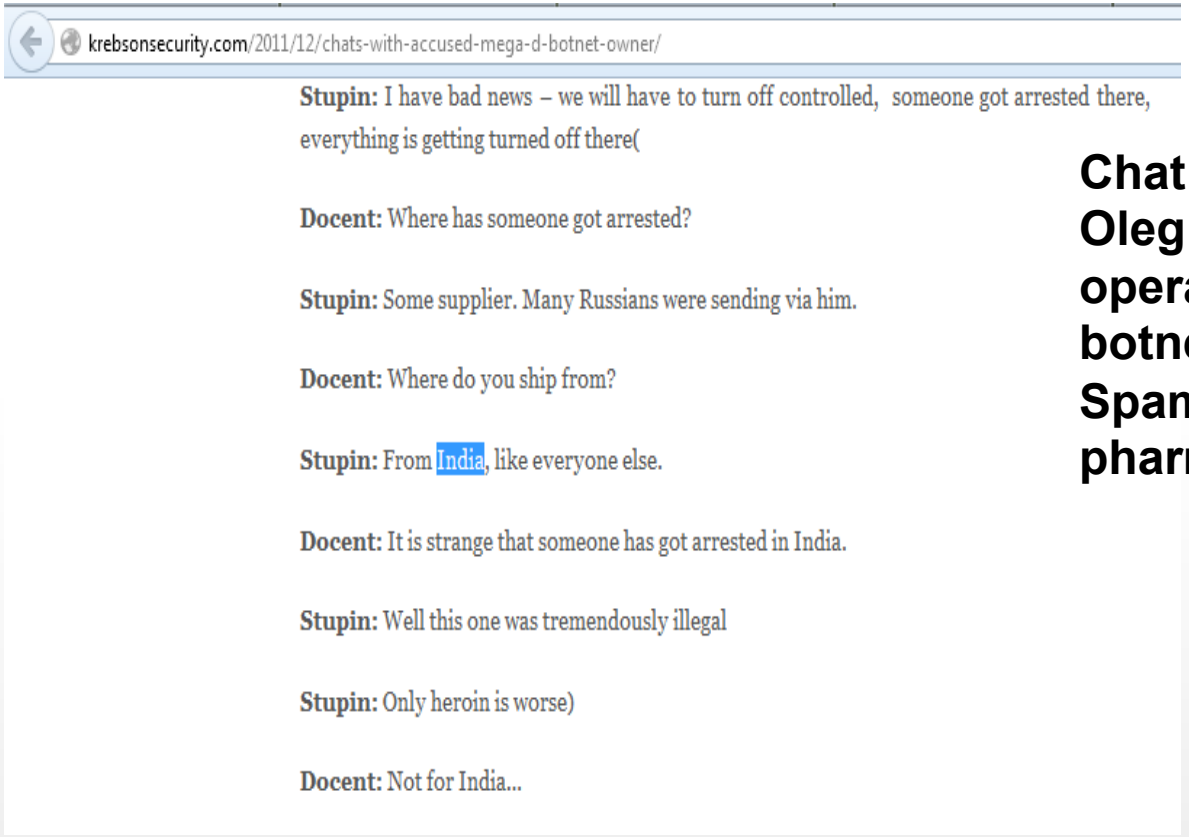
Just send Us Rs. 1000/- (USD 25) and we will send you the link to download the database.

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

M³AAWG
MESSAGING MALWARE MOBILE

India is a major part of the "supply chain" for pharmacy spam

M3AAWG
MESSAGING MALWARE MOBILE



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

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

M³AAWG
MESSAGING MALWARE MOBILE

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, 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>
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

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

The number of IPs blocked for virus traffic is huge

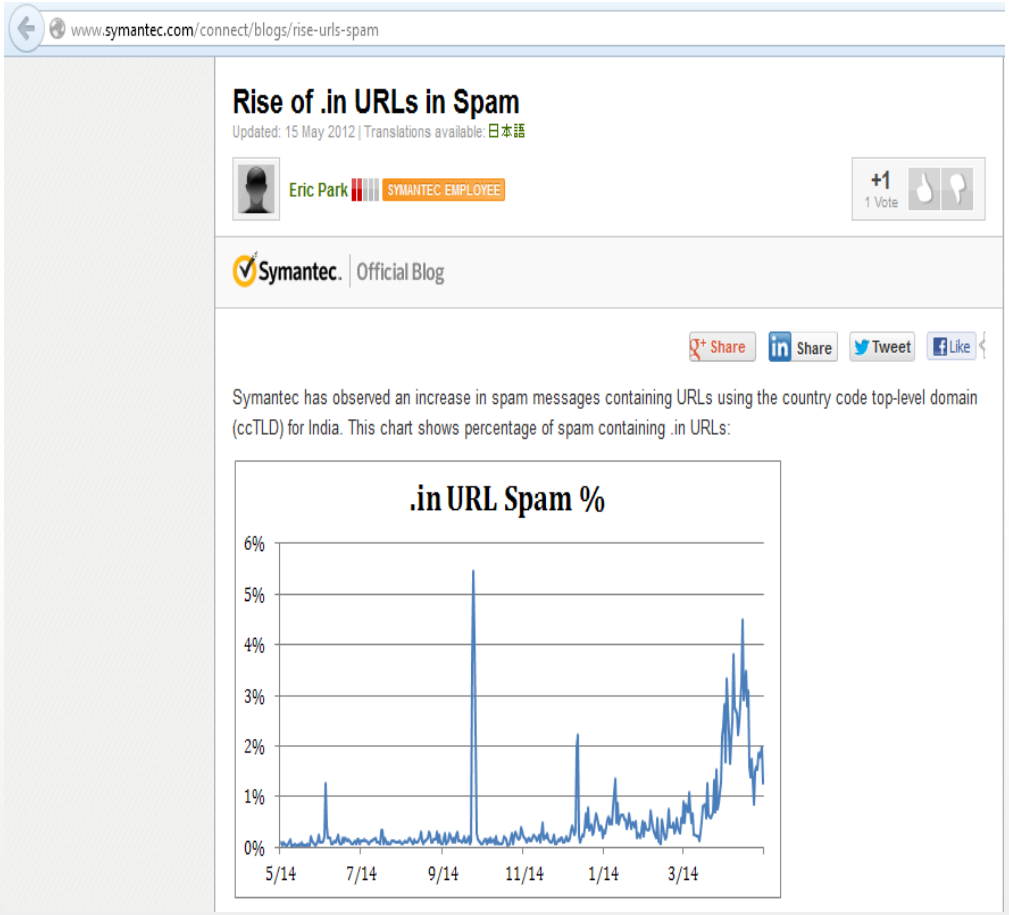
M3AAWG
MESSAGING MALWARE MOBILE

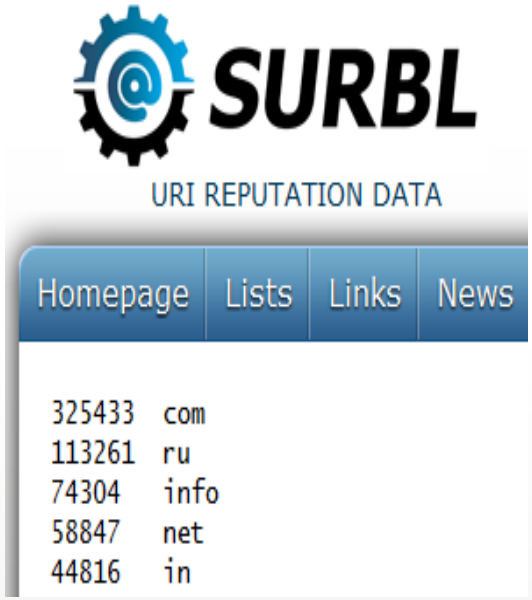
Extensive broadband penetration + insecure PCs = trouble

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

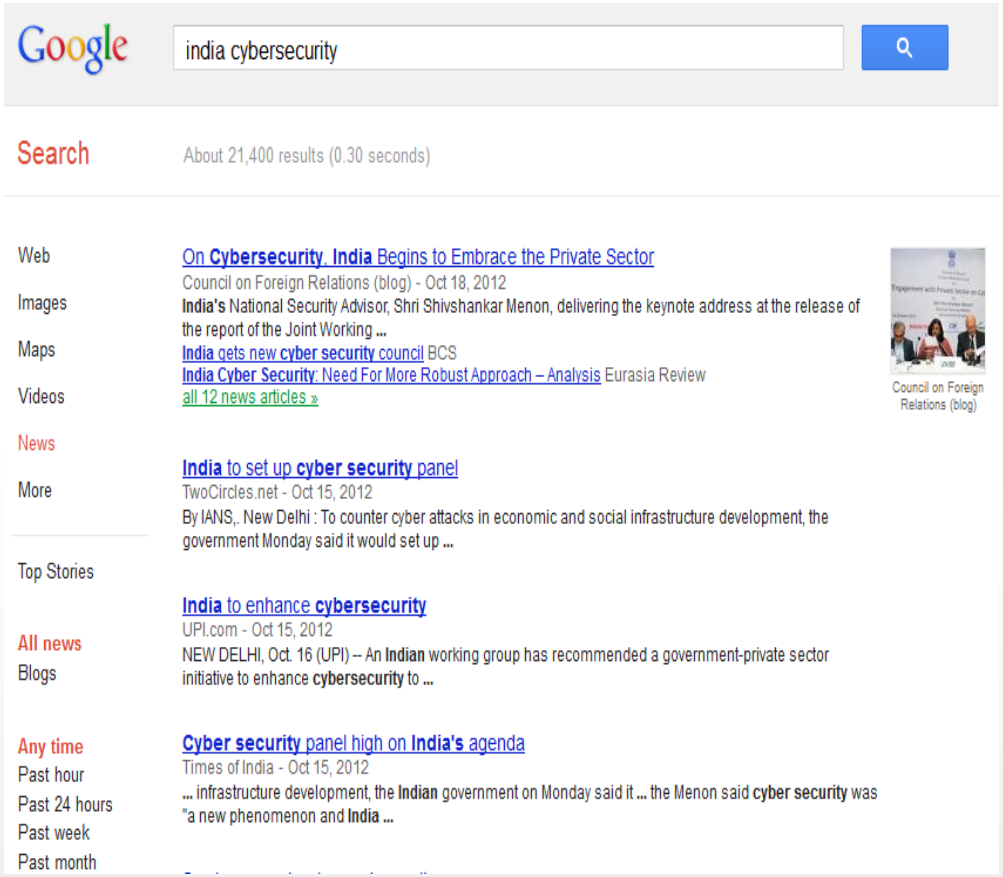




Courtesy Symantec and the SURBL Project

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

M³AAWG
MESSAGING MALWARE MOBILE



What can Indian ISPs do about messaging abuse?

M3AAWG
MESSAGING MALWARE MOBILE

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 M3AAWG members
- M3AAWG 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

M3AAWG
MESSAGING MALWARE MOBILE

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:

M3AAWG, APRICOT, SANOG

Local cooperation against spam and online threats

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

How Indian email marketers can help

- Adopt the M³AAWG 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

  M³AAWG, ESPC, and of course, IAMAI

Government & Law Enforcement - Suggestions

M3AAWG
MESSAGING MALWARE MOBILE

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, M3AAWG, OECD WPISP …

Localization of M³AAWG best practice documents

Several best practice documents published by M³AAWG 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.

M3AAWG
MESSAGING MALWARE MOBILE

Thank You