

The BRIC Countries and Online Abuse

Joe St Sauver, Ph.D.

joe@oregon.uoregon.edu

MAAWG Senior Technical Advisor

MAAWG 27th General Meeting
San Francisco, February 19-21, 2013

<http://pages.uoregon.edu/joe/bric/>

Disclaimer: all opinions strictly my own

What Are The BRIC Countries?

- Term coined in 2001 by Jim O'Neil of Goldman Sachs for four emerging economies -- Brazil, Russia, India and China – with tremendous potential power individually and as an economic bloc:
- Brazil and Russia: potentially dominant suppliers of **raw materials**
- China: potentially dominant supplier of **manufactured goods**
- India: potentially dominant supplier of **services**
- China and India also represent huge potential **consumer markets**
- Recent thinking, however, has begun to challenge the perception that the BRIC countries have a nearly inescapable economic destiny, see for example, "The Braking of the BRICs," Forbes, 5 October 2012, <http://www.forbes.com/sites/joelkotkin/2012/10/05/the-braking-of-the-brics/>
- **MAAWG cares about these countries for a more pragmatic reason, however -- their key roles in the abuse ecosystem**

Spam Bot Counts and the BRIC Countries

- The Composite Block List (CBL): The BRIC countries are prominently featured in the CBL, a list of known-botted IPs:

#1	China	1,894,140 IP addresses	30.11% of all listings
#2	India	706,693 IP addresses	11.93% of all listings
#5	Russia	223,893 IP addresses	3.78% of all listings
#8	<i>U.S.</i>	<i>115,640 IP addresses</i>	<i>1.95% of all listings</i>
#9	Brazil	109,381 IP addresses	1.85% of all listings

Source <http://cbl.abuseat.org/country.html> (11 Feb 2013)

(The U.S. is included (as a non-BRIC) for comparative purposes)

Note that the four BRIC countries collectively account for nearly half (47.67%) of all known bottled hosts worldwide.

(Most of the spam we all see gets delivered via bots)

Spamhaus Top 10 Worst Spam Countries

- The World's Worst Spam Producing Countries as of 2/20/2013:

#1	U.S.	3,174 current live spam issues
#2	China	1,323 current live spam issues
#3	Russia	983 current live spam issues
#7	Brazil	396 current live spam issues
#8	India	354 current live spam issues

- Source www.spamhaus.org/statistics/countries/
(The U.S. is included (as a non-BRIC) for comparative purposes)
- **Note that the four BRIC countries are top ten spam countries.**

Spamvertised Domains and the BRIC ccTLDs

- Domains in China's ccTLD (dot cn) were widely spamvertised until CNNIC cracked down on that practice in late 2009. When that happened, Russia's ccTLD, dot ru, became the preferred domain for pharma spammers and other abuse. (<http://krebsonsecurity.com/2010/03/spam-site-registrations-flee-china-for-russia/>)















- What do we see today? <http://www.surbl.org/tld> reports that on 11 Feb 2013, the TLDs with the most unique abused domains were:

383,045	com	[107,358,552 total domains]	3.567 per 1,000
118,824	ru	[3,790,000 total domains]	31.35 per 1,000
85,171	info	[7,236,224 total domains]	11.77 per 1,000
73,028	net	[15,020,071 total domains]	4.862 per 1,000
34,822	cn	[3,350,000 total domains]	10.39 per 1,000
22,546	in	[unknown]	[unknown]

- **Note that the dot ru abuse rate is ~10X worse than dot com...**

[total domains: www.whois.sc/internet-statistics/ http://centr.org/DomainWire_Stat_Report_2012_1 ; the total number of Indian domains isn't publicly disclosed, so rates can't be computed]

Banker Trojans: A Brazilian Specialty?

Malware Domain List							
www.malwaredomainlist.com/mdl.php?inactive=&sort=ASN&search=&colsearch=All&ascorder=DESC&quantity=100&page=2							
2011/05/30_19:30	depaulamdp.sites.uol.com.br/aut.jpg	200.147.33.19	200-147-33-19.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/05/30_19:30	tupinambamelosites.uol.com.br/Mouse.swf	200.147.1.41	200-147-1-41.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/06/01_18:59	kagiulietti.sites.uol.com.br/rodape.gif	200.147.33.21	200-147-33-21.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/06/07_20:09	miguelrubio.sites.uol.com.br/files.jpg	200.147.33.21	200-147-33-21.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/06/07_20:09	miguelrubio.sites.uol.com.br/aut.jpg	200.147.33.21	200-147-33-21.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/06/07_20:09	miguelrubio.sites.uol.com.br/okt.jpg	200.147.33.21	200-147-33-21.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/06/07_20:09	miguelrubio.sites.uol.com.br/ger.jpg	200.147.33.21	200-147-33-21.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/08/13_09:12	crogysz.sites.uol.com.br/moduloa.jpg	200.147.33.19	200-147-33-19.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/10/02_13:51	valdeilma.moraes.sites.uol.com.br/metodoS.swf	200.147.33.21	200-147-33-21.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/10/04_08:32	transrealtt.sites.uol.com.br/novobho/santa.gif	200.147.33.19	200-147-33-19.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/10/04_08:32	transrealtt.sites.uol.com.br/novobho/ne.gif	200.147.33.19	200-147-33-19.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/10/04_08:32	transrealtt.sites.uol.com.br/novobho/pegamsn.gif	200.147.33.19	200-147-33-19.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/10/04_08:32	transrealtt.sites.uol.com.br/novobho/gf.gif	200.147.33.19	200-147-33-19.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	
2011/10/04_08:32	transrealtt.sites.uol.com.br/novobho/lista.gif	200.147.33.19	200-147-33-19.static.uol.com.br.	trojan Banker	Contato Administrativo - UOL / l-registrobr-uol@corp.uol.com.br	7162	

(Alleged) Nation State Sponsored Attack Traffic

www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html

Chinese Army Unit Is Seen as Tied to Hacking Against U.S.



This 12-story building on the outskirts of Shanghai is the headquarters of Unit 61398 of the People's Liberation Army. China's defense ministry has denied that it is responsible for initiating digital attacks.

By DAVID E. SANGER, DAVID BARBOZA and NICOLE PERLROTH
Published: February 18, 2013 | [577 Comments](#)

On the outskirts of Shanghai, in a run-down neighborhood dominated by a 12-story white office tower, sits a People's Liberation Army base for [China's](#) growing corps of cyberwarriors.

[f](#) FACEBOOK

[t](#) TWITTER

[+](#) GOOGLE+

Other Abuse From The BRICs

Project Statistics | Project Honey Pot

<https://www.projecthoneypot.org/statistics.php>



Top-5 Countries For Harvesting
(see top-25)

#1		China (17.7%)
#2		Spain (15.8%)
#3		United States (10.3%)
#4		Romania (6.5%)
#5		Germany (4.2%)

Top-5 Countries For Spam Sending
(see top-25)

#1		China (10.0%)
#2		Brazil (8.9%)
#3		United States (7.1%)
#4		Germany (6.4%)
#5		Russia (6.0%)

Top-5 Countries For Dictionary Attacks
(see top-25)

#1		India (10.7%)
#2		Brazil (10.3%)
#3		Russia (6.5%)
#4		United States (5.1%)
#5		China (4.8%)

Top-5 Countries For Comment Spamming
(see top-25)

#1		United States (22.1%)
#2		China (18.2%)
#3		Russia (7.5%)
#4		Brazil (5.9%)
#5		India (5.7%)

Why?

- Corruption issues?
- Poverty?
- Language issues limiting security advice and localized tools?
- Something else?

Corruption Perceptions Index 2012

- Denmark: 1 (tie)
- Finland: 1 (tie)
- New Zealand: 1 (tie)
- United States: 19
- **Brazil: 69**
- **China: 88**
- **India: 94**
- **Russia: 133**
- Afghanistan: 174 (tie)
- Korea (North): 174 (tie)
- Somalia: 174 (tie)

Source: <http://www.transparency.org/cpi2012/results>

Nominal GDP Per Capita (UN 2011)

- Liechtenstein (#1): \$170,373
- Monaco (#2): \$167,021
- Luxembourg (#3): \$115,377
- United States (#18): \$47,882
- **Russia (#55): \$13,006**
- **Brazil (#58): \$12,594**
- **China (#93): \$5,439**
- **India (#143): \$1,528**
- Congo, Dem. Rep. \$237
- Somalia (#194): \$112

Source: http://en.wikipedia.org/wiki/List_of_countries_by_GDP_nominal_per_capita

Language Issues

- Users are more likely to secure their systems if you talk with them about system security in a language they understand!
- I know that I'd sure have a hard time understanding and following security advice offered to me only in Greek or Thai, neither of which I speak, rather than in English...

The Challenging Reality of Languages In India

- The (incorrect) stereotype is that most Indians speak Hindi (more accurate estimates peg that only at around 40%) or English (only a few percent of Indians are believed to actually use English, see for example <http://news.bbc.co.uk/2/hi/8365631.stm>).
- Many Indians use other, less-well-known, South Asian languages such Assamese (1.3%), Bengali (8.1%), Gujarati (4.5%), Kannada (3.7%), Maithili (1.2%), Malayalam (3.2%), Marathi (7%), Oriya (3.2%), Punjabi (2.8%), Tamil (5.9%), Telugu (7.2%), or Urdu (5%). (See: <http://www.cia.gov/library/publications/the-world-factbook/geos/in.html>). Of course, even a language that's used by "just" 1% of India's population still represents a language used by nearly 12 million people!
- For comparison, there were a little over 28 million Spanish-speaking people in the United States in 2000, and there are just under 7 million Canadians who speak French.

Offering Localized Security Advice Is One Thing, Localized Security Software' s Something Else

- It' s one thing to offer simple security advice in appropriate local languages, but are there alternative web browsers, antivirus products, and other critical security software available in fully internationalized formats to actually implement that advice?
- For example, checking www.mozilla.com/en-US/firefox/all.html I notice that Firefox is available in Assamese, Bengali, Gujarati, Hindi, Kannada, Malayalam, Marathi, Punjabi, and Telugu. Obviously that' s not every major Indian language, but it' s still a very nice start.
- On the other hand, if you want to get depressed, pick a major Indian language and try to find a commercial (or free) PC antivirus product that' s fully internationalized for that language. (Hint: some of the few products you may find may actually be malware, not anti-malware, so be careful out there!)