M^{3}AAWG
MESSAGING MALWARE MOBILE

Indian Service Providers and the Messaging, Malware, Mobile Anti-Abuse Working Group

Malware is one of the root causes of messaging and mobile abuse. International collaboration is the most effective strategy for curtailing the bots that attack end-users, harm ISPs and impede the global economy.

What are the issues for the Indian Internet service provider industry?

With over 17 percent of the world's population and rapidly expanding global fiber connectivity – as well as a pivotal role in the increasingly-influential BRIC (Brazil, Russia, India, China) economic block – India is a critical player in the Internet ecosystem. Unfortunately, as has been true for many other nations in the past, Indian Internet users and their service providers are being severely victimized by international cyber criminals.

Malware involuntarily installed on Indian end-users' computers turns those systems into spam-spewing bots from which cyber attacks can be launched against other users, India's own government, India's own critical infrastructure and even its allies' facilities. The presence of bots often results in overly broad blocks imposed against Indian Internet infrastructure and Indian Internet domain names, thereby causing substantial collateral damage to legitimate Indian Internet users and Indian companies.

The magnitude of this problem can be seen in the fact that India is currently #1 on the CBL list of botted countries with over 1.6 million (16 lakh) known spam bots.[1]

The *Times of India* reported on April 25, 2012 that 80 percent of the people surveyed in one study had experienced cyber crime.[2] If India is not able to effectively combat this abuse, it runs the risk of increasingly having its network traffic summarily rejected. This would jeopardize its ability to fully and profitably participate in the global Internet economy.

We recognize that Indian ISPs face some special challenges, particularly when it comes to the diverse languages used in the various regions of India.[3] Yet these challenges do not dispel the compelling need for effective action.

Although these problems are currently most-pressing on traditional computers systems, we note that India, as the country with the second or third largest number of known cell phone users in the world, does, or likely soon will, face comparable issues in the mobile space as well. This space is made doubly complicated by the need to comply with government requirements relating to lawful interception for national security purposes following the despicable 13/7 Mumbai bombings.

[1] See http://cbl.abuseat.org/country.html).

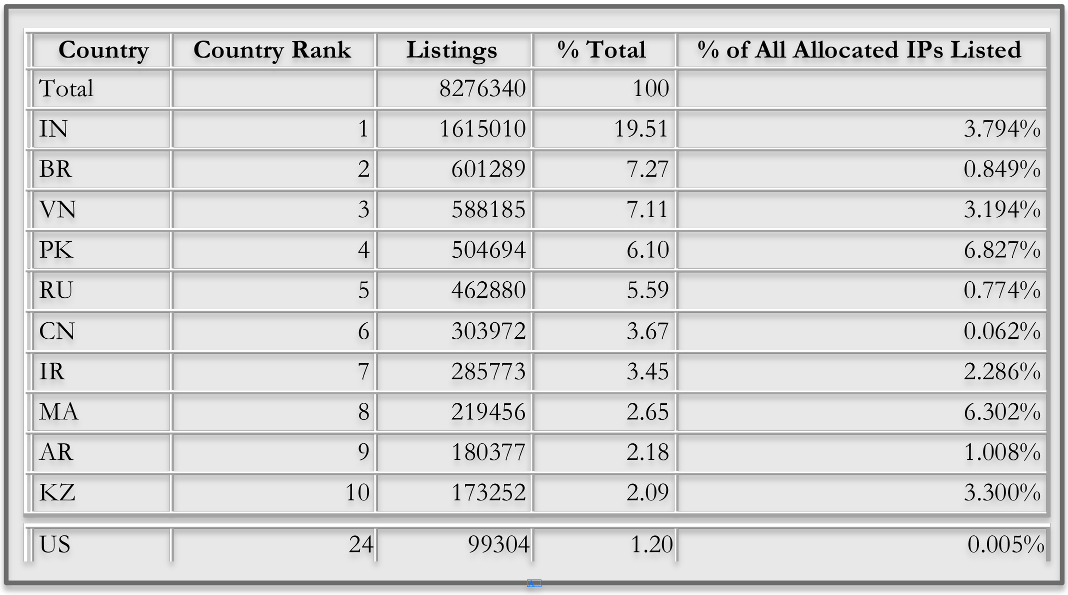
[2] See "133 govt websites hacked in Jan-Mar: Sachin Pilot" http://tinyurl.com/7gerpaj

[3] See "Beginning to Remediate Botted Hosts Abroad: India" http://tinyurl.com/6ndtwsj

CBL breakdown by Country, Highest by count

Date prepared: Fri May 18 00:45:38 2012 UTC/GMT

http://cbl.abuseat.org/country.html - Data used with the permission of the CBL.



Country	Country Rank	Listings	% Total	% of All Allocated IPs Listed
Total		8276340	100	
IN	1	1615010	19.51	3.794%
BR	2	601289	7.27	0.849%
VN	3	588185	7.11	3.194%
PK	4	504694	6.10	6.827%
RU	5	462880	5.59	0.774%
CN	6	303972	3.67	0.062%
IR	7	285773	3.45	2.286%
MA	8	219456	2.65	6.302%
AR	9	180377	2.18	1.008%
KZ	10	173252	2.09	3.300%
US	24	99304	1.20	0.005%

India is currently #1 on the CBL list of botted countries with over 1.6 million (16 lakh) known spam bots.
M^{3}AAWG promotes cooperative global efforts to tackle bots and malware on both fixed and mobile networks.

What impact can abuse have on revenue?

For ISPs that have been victimized, spam and other abuse is expensive in many different ways:

- **Direct Customer Care:** Users infected with malware often have systems that are slow or unstable, or they may be subjected to unwanted advertisements, or they might have their credentials stolen leading to identity theft. When these adversities occur, customers generally contact their ISPs. Each call can destroy the profitability of that customer for months, if not for years. Even simply licensing a software security suite for customers can reduce already-thin ISP margins.

- **Increased Customer Churn:** When systems are botted and acting badly, it is common for customers to blame their ISP and to hope that another ISP will provide a better experience. Every time customers leave their current ISP for an alternative one, it negatively impacts the losing ISP's bottom line. Eliminating bots on customer hosts can help ensure customers stay happy – and stay put.

- **Potential Regulation:** As in the United States or the European Union, to the extent that the Indian Internet service provider industry does not police itself, the Indian government may feel it has no option but to step in to do so, since citizens' safety and continued economic growth are at stake. Increasing regulation normally implies increasing ISP compliance costs. Self-regulation is thus generally viewed as a far better option.

- **Persistent Damage to Online Assets:** Once an ISP's address space is block listed, it can be extremely difficult or impossible to have it unlisted. In many cases, the ISP may not even know that its traffic is being silently black holed, making it virtually impossible to rehabilitate an IP address block once it has developed a bad reputation. In the old days, this was just an inconvenience for growing ISPs since old, heavily-blocklisted address blocks could be replaced with newly-obtained IP addresses. However, APNIC has now run out of IPv4 address space. This makes it all the more important to carefully guard the address space you currently have.

- **Bad Customers Drive Out Good Customers – and Attract More Bad Customers:** Once an ISP is victimized, good customers often become frustrated by being blocked or experiencing other issues and flee to less-infested, alternative ISPs. Who's left? The bad customers remain and, as word begins to spread, their undesirable friends join them. ISPs can easily end up getting sucked into an irrecoverable "death spiral."

What are the benefits for consumers and business customers in dealing with and rectifying abuse issues?

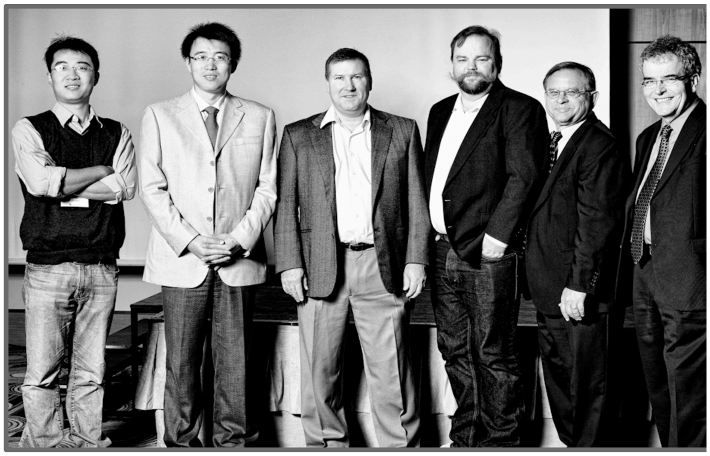
At one time, it was common for users of infected computers to say: *Why should I spend "my" time and "my" money cleaning up "my" computer so that "you" will not get spammed? What's in it for "me"?* Fortunately, most users now understand that malware infections can directly hurt them most of all. For example, banker trojans may lurk on a user's computer, just waiting to steal and send-off the user's credit card number, bank information, or user name and password. Or consider badly written malware that makes a system unstable and prone to crash, sometimes causing work to be irrecoverably lost. These days most users "get it" and understand that having good system hygiene is in their own self-interest and that it is also good for the Internet as a whole.

That said, there is still much work to be done. Many Indian Internet users remain infected and will need help to get disinfected and hardened against future compromises. We believe that ultimately Indian ISPs need to collaborate together with other global entities to effectively address the challenges they face. M^{3}AAWG is pleased to help and welcomes your input on India's interest in addressing these challenges.

London Action Plan (LAP) Executives with M^{3}AAWG Officers in Paris

What are the security benefits of participating in M^{3}AAWG?

The Internet security community is, by nature, a tight knit group. Who you know is often as important as what you know when it comes to receiving timely threat warnings and developing direct channels for resolving incidents. M^{3}AAWG meetings and activities are packed with some of the most influential security and anti-abuse colleagues in the world, and those contacts, combined with documented best practices and M^{3}AAWG training, can help key personnel at participating ISPs avoid hidden landmines that might otherwise prove very costly for their companies.



Chinese Internet executives with M^{3}AAWG officers. The EastWest Institute chose to announce the first China-U.S. report on efforts to control spam at a M^{3}AAWG meeting.

What are the benefits to the companies that participate in the M^{3}AAWG process?

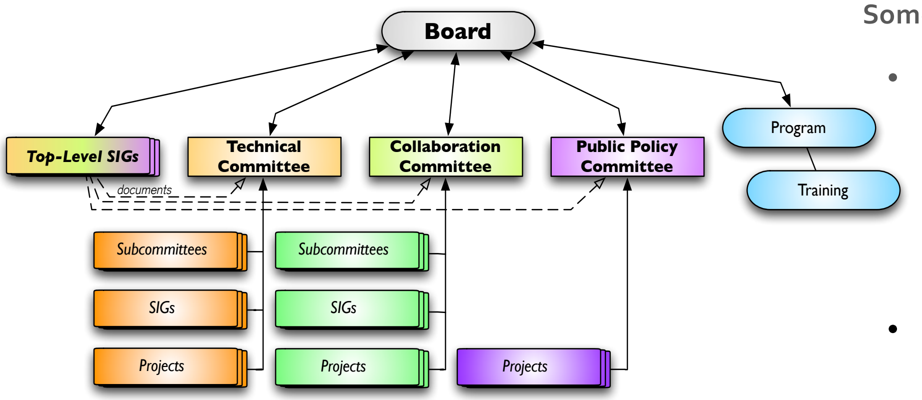
M^{3}AAWG is recognized as the leading, neutral global forum where major service providers, mobile network providers, public policy advisors, anti-abuse vendors and volume senders can work together to jointly solve abuse-related problems of mutual interest. In the process of developing industry best practices and documents, M^{3}AAWG members have access to a closed, confidential forum for sharing key information among companies. This candid exchange often leads to resolving many of the pressing problems currently bedeviling the online community. M^{3}AAWG also works to ensure that industry concerns are effectively voiced with governments, public policy agencies, Internet governance bodies and NGOs. We do not lobby but we are recognized as a technology-neutral, non-political working body that advises legislators and regulators on the technical consequences of legislation and regulatory action.

Who attends M^{3}AAWG? What are the typical job titles of attendees?

Typical titles for attendees are Director of Anti-Abuse at network operators, Director of Security, Chief Technology Officer, Distinguished Engineer, Engineering Fellow, Vice President of Messaging, Vice President of Public Policy, and Chief Scientists. The overall attendance is operational and security management at the director level, technical experts and senior policy directors.

How is the organization structured and who is its leadership?

M^{3}AAWG Organizational Structure



A brief overview of M^{3}AAWG membership:

M^{3}AAWG covers more than one billion inboxes with 200 members worldwide, including major ISPs, telecommunications and mobile operators, email providers, anti-abuse vendors and social media companies.

- Major ISPs, telecommunications companies, email providers such as 1&1 Internet AG; AOL; AT&T; Bell Canada; Charter Communications; Comcast; Cox Communications; France Telecom; Google; Microsoft; Sprint; Swisscom; TDC; Telenet N.V.; Telefonica S.A.; Time Warner Cable; T-Mobile US; Verizon; UPC Broadband Operations BV; and Yahoo!
- Social networking companies, and major brands including Amazon Web Services, Facebook, LinkedIn; and Zynga, Inc.
- Financial services like La Caixa, PayPal; and Visa Europe
- All the major anti-virus and security vendors including BAE Systems Detica; Cloudmark; eleven GmbH; F-Secure Corp.; Kaspersky Lab; McAfee; Sophos Plc; Symantec; and Trend Micro
- Leading hardware and software vendors such as Apple, Cisco, and HP
- International anti-abuse organizations, such as CAUCE; eco, an association of German ISPs; NCTA; Spamhaus; Shadowserver; and SURBL

Questions? Want to join us?
Contact: Jerry Upton, M^{3}AAWG Executive Director
jerry.upton@m3aawg.org

Some of the M^{3}AAWG Chairmen Affiliations:

- **Michael O'Reirdan, M^{3}AAWG Co-Chairman, Malware**, has addressed OECD on the alarming rise of the botnet and malware threat and chairs the U.S. Federal Communications Commission CSRIC Working Group #7, which recently issued the U.S. Anti-Bot Code for ISPs.
- **Chris Roosenraad, M^{3}AAWG Co-Chairman, Messaging**, is an advisor on fighting online child exploitation at ICMEC (International Center for Missing and Exploited Children).
- **Alex Bobotek, M^{3}AAWG Co-Chairman, Mobile,** is active in the GSMA Security Group, the OMA (Open Mobile Alliance), and other groups. He has addressed China National Computer Network Emergency Response Team (CNCERT) and frequently addresses industry conferences on mobile abuse issues.

More information:

Detailed committee information is at
www.m3aawg.org

A complete member listing is at
http://www.m3aawg.org/about/roster/

A list of published documents is available at
http://www.m3aawg.org/published-documents

M^{3}AAWG public policy comments are at
http://www.m3aawg.org/activities/published-comments

M^{3}AAWG Email Metrics Reports are available at
http://www.m3aawg.org/email_metrics_report

Upcoming meeting dates and locations are at
http://www.m3aawg.org/events/upcoming_meetings

M^{3}AAWG YouTube channel:
https://www.youtube.com/user/MAAWG/videos

M^{3}AAWG Facebook Page:
www.facebook.com/maawg

M^{3}AAWG on Twitter: www.twitter.com/maawg

M^{3}AAWG
MESSAGING MALWARE MOBILE
Messaging^3 Anti-Abuse Working Group
San Francisco, CA 94129-0920 U.S.A. ■ www.M3AAWG.org

Updated May 2012