# ITU Botnet Mitigation Toolkit

## Background Information

ICT Applications and Cybersecurity Division
Policies and Strategies Department
ITU Telecommunication Development Sector

January 2008

International
Telecommunication
Union

## *Acknowledgements*

Botnets (also called zombie armies or drone armies) are networks of compromised computers infected with viruses or malware to turn them into “zombies” or “robots” – computers that can be controlled without the owners’ knowledge. Criminals can use the collective computing power and connected bandwidth of these externally-controlled networks for malicious purposes and criminal activities, including, *inter alia*, generation of spam e-mails, launching of Distributed Denial of Service (DDoS) attacks, alteration or destruction of data, and identity theft. The threat from botnets is growing fast. The latest (2007) generation of botnets such as the Storm Worm uses particularly aggressive techniques such as fast-flux networks and striking back with DDoS attacks against security vendors trying to mitigate them. An underground economy has now sprung up around botnets, yielding significant revenues for authors of computer viruses, botnet controllers and criminals who commission this illegal activity by renting botnets.

In response to this growing threat, ITU is developing a *Botnet Mitigation Toolkit* to assist in mitigating the problem of botnets. This document provides background information on the toolkit. The toolkit, developed by Mr. Suresh Ramasubramanian, draws on existing resources, identifies relevant local and international stakeholders, and takes into consideration the specific constraints of developing economies.

The toolkit has particularly benefited from the input and comments of many people to whom we owe our thanks. Among others, we would like to thank Robert Shaw, Head of the ITU’s ICT Applications and Cybersecurity Division, for initiating the project, Bruce Matthews, Chris Duffy and Kayne Naughton (ACMA, Australia), Anne Carblanc, Audrey Plonk and Claudia Sarrocco (OECD), Jean-Jacques Sahel, (BERR, UK), and members of the StopSpamAlliance.org dynamic coalition. Additionally, we would like to thank Yat Siu, Tony Basoglu and Ibrahim El-Mouelhy (Outblaze), Joe St. Sauver (University of Oregon), David Allen (Collab CPR), Anne Carblanc, Audrey Plonk and Claudia Sarrocco (OECD), Jean-Jacques Sahel, (BERR, UK), Barry Raveendran Greene (Cisco), Ken Simpson (MailChannels), David Dagon (Georgia Tech), Dave Crocker (Brandenburg InternetWorking), Chris Lewis (Nortel) and  Danny McPherson (Arbor Networks). Finally, thanks go to Christine Sund (ITU) as well as to Sarah Roxas (ITU) for the design of the toolkit layout and related web pages.

The *ITU Botnet Mitigation Toolkit* a project of the ITU Telecommunication Development Sector’s ICT Applications and Cybersecurity Division. It is part of a broad range of activities promoting cybersecurity and critical information infrastructure protection.

The latest version of the *ITU Botnet Mitigation Toolkit* and related resources are available at:

http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

For further information on the toolkit, please contact:

ICT Applications and Cybersecurity Division (CYB)
Policies and Strategies Department
Bureau for Telecommunication Development
International Telecommunication Union
Place des Nations
1211 Geneva 20
Switzerland

Telephone: +41 22 730 5825/6052
Fax: +41 22 730 5484
E-mail: cybmail@itu.int
Website: www.itu.int/ITU-D/cyb/

# Table of Contents

# Executive Summary

'Botnets', or as the media calls them, 'Zombie Armies' or 'Drone Armies', and their associated  malware have grown over the years into a multimillion dollar criminal economy, a risk to government, critical infrastructure, industry, civil society and to the broader Internet community.

Botnets are coordinated groups of several (tens, hundreds or even thousands of) computing devices such as PCs, laptops and even the new generation of mobile devices such as 'smartphones', all infected with the same virus or other malware.

Their collective computing power and Internet connectivity is pooled together and remote controlled for the performance of malicious and criminal activities ranging from spam and identity theft to espionage and coordinated attacks on a country’s critical infrastructure and Internet resources.

This toolkit presents a broad set of approaches that can be followed by a variety of stakeholders spread across Government, Industry and Civil Society.  There are initiatives that call for broad-based cooperation at local, regional and international levels, across stakeholder communities.

The parts of the toolkit mesh closely with each other, and are envisaged as part of an overall strategy for botnet mitigation.  A detailed treatment of various aspects of this toolkit is split into individual appendices for policy, technical and social measures.  Individual sections may describe efforts specifically targeted at a particular stakeholder community, but which other communities involved in this effort would be made aware of, at least in a summary form.

Given the broad scope and the broad-based target audience of this paper, some sections of the paper may be especially relevant to one community of stakeholders, while being of, at the most, broad interest to other communities that would not require the technical minutiae relevant to the target community.

The initiatives described in this paper are a mixture of short and long term measures, which need to be pushed forward, with coordination between the initiatives and their implementing organizations, but also with all possible care taken to ensure that one initiative lagging behind does not impede the progress of other related or unrelated initiatives.

Emphasis will be placed on capacity building, international cooperation and outreach – which are quite frequently the main inhibitors of such initiatives in developing economies, with resource shortages possible to at least partially be worked around by the provision of locally available and cost effective alternatives to more mainstream but costlier resources.

Several international organizations around the world (including the APEC-TEL/OECD working group on malware, the OECD task force on spam, as well as industry and civil society groups such as MAAWG, APWG, and others) have established a broad base of existing resources and documentation on social, technical and policy initiatives intended to mitigate the inter-related problems of spam and malware.

There is a sufficiency of best practice documents, task force and working group reports, etc. that cover a very broad spectrum of stakeholders and goals. This paper attempts to condense these efforts, and make the best possible use of prior work, with due acknowledgment, towards the goal of mitigating botnets and malware, particularly in developing economies.

The paper also focuses on building links with existing efforts in the area of spam, botnet and malware mitigation, in order to extend the benefits of such initiatives to developing economies, either in the form of (if necessary, translated) best practice and other documents, or in the form of assistance with training and if possible, resources.

The ideas presented and measures identified in this program will be the subject of ongoing country level pilot projects that will involve a broad base of relevant local stakeholder communities within a country, as well as facilitate to some extent the engagement of these stakeholders with similar efforts on a regional and international scale.

# The Threat Picture

Botnets are an illegal and unethical application of the concept of Distributed Systems, which has existed since at least 1970, in which multiple computing devices cooperate to achieve an integrated result. A variant of this concept, developed in the late 1990's, involves owners of Internet connected devices voluntarily donating their spare computing power and bandwidth to legitimate projects.

One of the earliest such global distributed systems projects is BOINC[1], the Berkeley Open Infrastructure for Network Computing, originally developed at the University of California, Berkeley to support the SETI@home[2] project that attempts to locate extra terrestrial intelligence, and has since been used in molecular biology, mathematics and astrophysics.

The most obvious difference between a botnet and a voluntary distributed systems project is consent – people who participate in projects like SETI@home do so out of an active interest in contributing to the project's goals, and voluntarily donate their computing power by downloading and running a screen saver or other BOINC client software onto their computers.

Botnets, on the other hand, are maliciously created by infecting unwitting users' computing devices with malware, entirely against their consent, and then remote controlling these compromised hosts to make them collaborate on a wide variety of nefarious tasks.

Distributed Systems, and even more so, Botnets, can claim a significant edge in processing power over traditional supercomputers, at a negligible fraction

[1] http://boinc.berkeley.edu
[2] http://setiathome.berkeley.edu/

of the cost.  The botnet, like a parasite, thrives on computing and bandwidth resources stolen from infected hosts.

The most powerful supercomputer currently in operation[3], the BlueGene/L system being developed by IBM and the US Department of Energy's National Nuclear Security Administration, and installed at the Lawrence Livermore National Laboratory, was benchmarked at 280.6 Teraflops (280.6 x $10^{12}$ Floating Point Operations Per Second).

At the time of writing (July 2007), BOINC has 588,403 active hosts out of 2,043,449 participating hosts generating a total computing power of almost double that of BlueGene/L: 560.188 Teraflops.[4]

***In comparison, Botnets of over 1.5 million active hosts[5] have been reported - a malicious distributed computing network that is over three times the size of BOINC.***

Botnets are a worldwide menace, widely used by spammers and cyber criminals. The use of botnets for cybercrime has increased and become even more refined since 2002-3 when the first mass mailer worms such as Sobig and Sober were released.

A complex and illegal underground economy has grown around the nexus between spammers, "Botherders" and malware authors, with traditional organized criminal gangs, using the following scenario:

- Spam is one of the primary vectors to distribute malware;
- Malware is used to compromise computing devices and create botnets, which are used for online crime;
- Organized criminal gangs launder the proceeds from online crime, and profits finance further software development efforts in malware and botnet development.

[3] http://www.top500.org
[4] http://www.boincstats.com
[5] http://informationweek.com/story/showArticle.jhtml?articleID=172303265

This underground economy serves to extend and broaden the reach of traditional crimes, so that some purely local criminal activities can now exploit the worldwide reach of the Internet.

The most visible use of botnets is the emission of spam and malware, which has captured the attention of policymakers and ISPs around the world and engendered various attempts to mitigate spam and malware traffic, most commonly by restricting port 25 (SMTP) outbound traffic.

However, the damage potential of a botnet is much more extensive - spam and malware emission is just the tip of the iceberg, and attempting to combat botnets simply by blocking port 25 has been compared, colorfully (and validly) by one expert to “treating lung cancer with cough syrup” [6].

Botnets have been used to launch DDoS attacks on entire countries and on critical Internet infrastructure – such as a recent attack that targeted the root servers[7], attacks on various spam blocklist providers such as Spamhaus.org, or the coordinated denial of service attacks on Estonian Internet sites[8] in May 2007 – the Estonian DDoS attacks were sourced from more than 560 unique networks located in over 50 countries.

In addition to spontaneous expression of nationalistic sentiments by botnet operators (such as those that apparently triggered the Estonian DDoS attacks), botnets are increasingly being used by criminals to attack the election campaigns and websites of various politicians.

The motivation for such activity is unknown, but could range from a criminal’s own political preferences to their being paid to launch botnet campaigns for or against a politician.

A spam campaign[9] promoting US Presidential candidate Ron Paul lasted from October 27 to 30, 2007, and was traced back to a Russian botnet spam

[6] http://darkwing.uoregon.edu/~joe/port25.pdf
[7] http://www.icann.org/announcements/announcement-08mar07.htm
[8] http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/
[9] http://www.secureworks.com/research/threats/ronpaul/?threat=ronpaul

operation called “Elphisoft”, which used a botnet-based spam tool called “Reactor” and the “Snizbi” trojan.  In those three days, around 3,000 bots were used to send out email to 162,211,647 email addresses.   The Ron Paul campaign has denied sending this spam.

Russian and Ukrainian political websites also appear to be targeted by botnet launched DDoS attacks – including a website belonging to former world chess champion and political activist Garry Kasparov[10]..

Extortionists routinely threaten to launch DDoS attacks or hack into a business’ website or e-Commerce portal if a ransom is not paid.  In October 2006, three Russian nationals were sentenced[11] to eight years in prison for extorting millions of dollars from sports betting firms by using botnets to launch DDoS attacks against them.

Botnets are widely used for a multitude of illegal and fraudulent activities. In addition to hosting entire phishing campaigns (spam emitters, DNS and web servers for phish websites), they are used to mine infected PCs for credit card information, passwords and other personally identifiable information such as passport numbers, names and addresses, in order to commit identity theft.

They are used in industrial espionage, extortion, data theft, password cracking and decryption of cryptographic keys and ciphers used for corporate systems and network security.  Illegal content such as child pornography is routinely distributed using botnet hosted websites and P2P networks.

# Lack of Coordination among Stakeholders

The botnet problem (like the spam problem) is the same problem worldwide, but is particularly acute in emerging Internet economies, owing to resource

[10] http://asert.arbornetworks.com/2007/12/political-ddos-ukraine-kasparov/
[11] http://www.kommersant.com/page.asp?id=709912

scarcity and capacity issues.  Government, industry, and civil society in emerging Internet economies are often ill equipped to deal with the catastrophic effects of botnets.

This results in a massive loss in confidence and perception of a lack of security in the use of ICTs and is one of the primary concerns raised during the World Summit on the Information Society (WSIS) process, which was sought to be addressed in follow-up to WSIS Action Line C5.

There is a multiplicity of different initiatives to mitigate botnets, several of which operate on broadly similar lines.  This leads to a substantial amount of duplicated effort and diverse, disparate data sources.

In general, groups of related stakeholders tend to congregate in what can be described as stakeholder communities. Stakeholder communities may be formed based on geography, shared membership in an International organization, or based on the roles and functions of the participating stakeholders.

Therefore groups have formed that are focused solely on Europe or on the Asia Pacific region, and other groups have formed to bring together civil regulators, law enforcement agencies, ISPs or civil society organizations.

These communities tend to operate in completely different and siloed spheres, with relatively limited awareness, formal coordination and communication between different communities.  In cases where awareness or channels of communication do exist, these are typically informal, for example where a single organization may participate in more than one stakeholder community.

In general, there is need for coordination between groups across multiple stakeholder communities, to establish broad consensus on botnet mitigation. Groups involved in botnet mitigation may find it expedient to cooperate, in order to establish joint work programs or organize collocated meetings.

Such coordination cutting across stakeholder communities does exist, and has been found to be remarkably productive in the cases where it is to be found.

National public-private partnerships such as the Australian Communications and Media Authority's “Australian Internet Security Initiative” (AISI) have been formed to address botnets, malware and other cybersecurity related issues.

Further, there is extensive cooperation between international organizations, for example, the joint work on malware[12] by the Organization of Economic Cooperation and Development (OECD) Working Party on Information Security and Privacy (WPISP) and the Asia Pacific Economic Cooperation Telecommunication and Information Working Group (APEC-TEL) Security and Prosperity Steering Group (SPSG).

Additionally, industry and technical expert coalitions such as the Messaging Anti-Abuse Working Group (MAAWG)[13] and the Anti Phishing Working Group (APWG) [14] are active in this space. NSP-SEC[15] is a loose network of network security personnel at ISPs around the world, focused on operational mitigation of botnets and other Internet security threats.

[12] http://www.oecd.org/document/34/0,3343,en_2649_34223_38293474_1_1_1_1,00.html
[13] http://www.maawg.org
[14] http://www.apwg.org
[15] http://www.nspsec.org

# The Botnet Economy

In contrast, stakeholders on the other side of the equation actively collude with each other and are much quicker at forming relationships, unburdened by formal processes and protocol and driven to cooperate based on a common goal – “Other People’s Money”.

Because botnets are associated with substantial illegal revenue, a thriving underground economy has sprung up around botnet activity.

A comprehensive study on the underground Botnet economy is “An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants”[16] by J. Franklin, V. Paxson, A.Perrig and S.Savage, Proc ACM CCS, October 2007. Other papers of interest on this subject include:

- Studying Malicious Websites and the Underground Economy on the Chinese Web[17], by Jianwei Zhuge; Thorsten Holz; Chengyu Song; Jinpeng Guo; Xinhui Han; Wei Zou, Universität Mannheim;
- “The Underground Economy - Priceless”[18], by Rob Thomas, Team Cymru,
- “The Commercial Malware Industry”[19], by Peter Gutmann, University of Auckland.

There are three main types of miscreants that are involved in the botnet economy: **malware authors** write and release malware; **botherders** run the botnets, operating them through ‘command and control’ channels; and **clients** commission new malware development or botnet activity in order to accomplish criminal objectives such as spam, identity theft, DDoS attacks, etc.

[16] http://www.cs.cmu.edu/~jfrankli/acmccs07/ccs07_franklin_eCrime.pdf
[17] http://madoc.bib.uni-mannheim.de/madoc/volltexte/2007/1718/
[18] http://www.usenix.org/publications/login/2006-12/openpdfs/cymru.pdf
[19] http://www.cs.auckland.ac.nz/~pgut001/pubs/malware_biz.pdf

There is increasing evidence that organized crime gangs are involved in all stages of the botnet economy, from writing malware and launching botnets to laundering money stolen or extorted from victims of botnet activity. Online criminals routinely use standard money laundering tactics such as the use of “mules” and “drops”, as well as electronic fund transfer and offshore banking services for quick movement of money between countries.

Despite this ostensible cooperation, “competition” within the botnet economy is quite vicious – some botherders will attack other bot networks and try to take them over, an option that is easier and more cost effective for them than building a botnet from scratch. Some botnets, such as those created by the Storm Worm, will launch DDoS attacks against competing bots[20], as well as against suspected honeypots or any other computer that attempts to scan the botnet.

Communication within the botnet economy takes place through heavily restricted access IRC and IM chat rooms, forums, and other communication means. Strong cryptography is used to encrypt email or other communications, and these may further be routed through a chain of botnet hosts, using email accounts bought using fake identities and stolen credit cards. Existing members of botnet gangs extensively vet new entrants before allowing them to join these closed forums.

The highly illegal and viciously competitive nature of the botnet underground economy has led to the development of a well developed system of self-regulation and policing to identify and launch counter attacks on “bad actors” (a catch-all term for fraudsters who try to cheat other fraudsters, undercover law enforcement or security employees, etc).

There is a potential threat to the physical security of individuals engaged in anti-botnet research and take down, as well as their families.

[20] http://asert.arbornetworks.com/2007/07/when-spambots-attack-each-other/

Given the strong links to organized crime, the current trend of launching DDoS attacks against opponents may potentially be supplemented, or even replaced, by physical assault and intimidation. Several mailing lists and research groups focused on botnets have criteria in place to vet potential members before their being allowed to join these groups.

# The ITU Botnet Mitigation Toolkit

This is a background paper for the entire toolkit and briefly describes a multi-pronged, multi-stakeholder strategy for Botnet Mitigation, with a particular focus on enabling developing economies to effectively mitigate the effect of Botnets on their economies and societies.

The paper focuses on a derivative application of the work already undertaken by these groups as well as previous initiatives such as the OECD Task Force on Spam, and intends to develop a “Botnet Mitigation Toolkit” – a multi-stakeholder, multi-pronged approach to track and mitigate the impact of botnets, with a particular emphasis on problems specific to emerging Internet economies.

This package will broadly parallel approaches recommended by the OECD Anti-Spam Toolkit for the definition of the problem space and suggested categorization of solutions.

This paper supplements and complements other cybersecurity-related activities being undertaken in the International Telecommunication Union Telecommunication Development Sector. For example, the ITU Development Sector (ITU-D)’s Study Group 1, through work on Question 22/1 is developing a *Report on Best Practices for a National Approach to Cybersecurity*. This report outlines a *Framework for Organizing a National Approach to Cybersecurity*. A related toolkit, the *ITU National Cybersecurity/CIIP Self Assessment Toolkit*[21] is intended to assist national

[21] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html

governments in examining their existing national policies, procedures, norms, institutions, and relationships in light of national needs to enhance cybersecurity and address critical information infrastructure protection.

The methodologies proposed in the paper are selected to be scalable, with the highest possible return on investment in financial, human and capacity resources.

Unique conditions particular to emerging Internet economies (such as a lack of regulation and resource scarcity) are kept in mind when customizing existing approaches to mitigation.

The goal is to use or recycle locally available resources as much as possible, and to select approaches based on the lowest possible cost combined with the highest degree of flexibility.

Stakeholders at the local level will be involved from government, industry and civil society to tailor and customize solutions to suit a broad spectrum of local conditions.

Additionally, efforts will be made to foster local, regional and international cooperation across multiple stakeholder groups from Government, Industry and Civil Society that have a stake in botnet mitigation, bringing them together with subject matter experts with practical experience in this field.

# Components of the Toolkit

## *Broad Overview*

- Multi-stakeholder, multi-pronged approach, use of public private-partnerships
- Awareness and reuse of existing initiatives and structures in this arena
- Combination of top-down and grassroots, local, and international initiatives

## *Policy*

### Effective Antispam and Cybercrime Laws and Regulation

1. Dedicated laws on cybercrime
2. Adapted to the paperless and cross-border nature of Internet crime
3. Cross border jurisdiction established using a “country link” concept

### Capacity Building among relevant policy stakeholders

1. Training programs for regulators, law enforcement and judiciary
2. Briefings for lawmakers, ministry officials
3. Building a pool of trained investigators
4. Providing the required tools for cybersecurity, forensic analysis

### Comprehensive framework for international cooperation and outreach

1. Common and harmonized policy and enforcement mechanisms
2. Need for fast, coordinated action in cross border cases
3. International conventions and groupings on spam and cybercrime

### Conflicts between cybercrime and privacy legislations

1. Widely different privacy legislation and data sharing constraints
2. Activist privacy litigation increases levels of privacy and anonymity

### Framework for local enforcement of Cybercrime and Botnet Mitigation

1. ITU-D SG-1 Question 22/1 *Report on Best Practices for a National Approach to Cybersecurity* containing the *Framework for Organizing a National Approach to Cybersecurity* and the element on deterring cybercrime.
2. Development of watch, warning and incident response
3. Nodal agency as facilitator and information clearinghouse

## *Technical*

### Tools and techniques to identify and gather information about active botnets

1. Identification of IP space controlled by an ISP, for incident response
2. Maintenance of Whois and Rwhois records by ISPs
3. Automated detection and reporting of botnet hosts.
4. DNSBLs, honeypots, darknets, passive DNS, traffic flow based and log analysis techniques

### ISP best practices to mitigate botnet activity

1. Firewall and security policy changes at the network level
2. Port 25 management, walled gardens to quarantine infected users
3. Inbound and outbound email filtering
4. Authentication and Reputation systems
5. *Report as Spam* buttons an industry/community-wide watch, warning and incident response system
6. Distribution of secure ICT infrastructure to users

### Registrar and registry best practices to mitigate botnet activity

1. Detection and takedown of malware or botnet domains
2. Mitigation of fast flux DNS techniques used by botnets
    - Balancing whois privacy with enforcement needs

### Capacity building for e-commerce and online transaction providers

1. Technical measures (DDoS and data breach mitigation, authentication)
2. Procedures to detect and mitigate fraudulent transactions
3. Customer education and protection campaigns

## *Social*

### Broad based education initiatives on Internet safety and security

1. Target locations with large numbers of computer users – schools, cybercafés, etc.

2. Supplement and cooperate with existing civil society ICT initiatives

3. Use rich visual media (ads, cartoon strips, etc.) to simplify the message

### Facilitation of secure ICT access for users

1. Deploy secure Customer Premises Equipment (CPE) (such as secured and firewall enabled broadband routers and wireless access points) in homes, cafés and community networksdeploy secure CPE in homes, cafés and community networks

2. Work with newspapers, schools, ISPs to distribute security software

3. Suggest and encourage alternatives to software piracy (cheaper and/or open source software alternatives to commonly pirated software)

# Annex A – Policy

## *Effective Antispam and Cybercrime Laws and Regulation*

Several countries do have computer crime laws that make unauthorized access and use of third party computing resources illegal. Early litigation in the United States of America has made use of more traditional legislation based on the doctrine of Trespass to Chattel[22], in particular various early cases on spam, the use of crawler bots and hacking.

It is however widely recognized that specific computer crime laws need to be drafted that more appropriately address the complexity and unique nature of Internet crime. In addition, the rules of evidence may require modification to accept digital and other "non paper" data as evidence, and provide for methods such as digital signatures to authenticate and validate content.

The global, converged nature of the Internet quite frequently results in cases that require cross-jurisdictional cooperation measures. For example, forensic evidence relating to a botnet used to propagate spam or steal credit cards may be spread across several different countries.

A primary consideration for legislation is establishing jurisdiction, for example by introducing the concept of a "Country Link" to decide what cases fall within the jurisdiction of the country implementing the law. For example, the Australian Spam Act of 2003 introduces the concept of an "Australian Link". A message has an Australian link if it either originates or was commissioned in Australia, or if it originates overseas but was sent to an address accessed in Australia. In addition to the *Annex on Deterring*

[22] CompuServe v. Cyber Promotions (S.D. Ohio 1997) 962 F.Supp. 1015; Hotmail Corporation v. Van$ Money Pie (N.D.Cal. 1998); America Online v. IMS (E.D.Va. 1998) 24 F.Supp.2d 548; and eBay Inc. v. Bidder's Edge, Inc. (N.D.Cal. 2000) 100 F.Supp.2d 1058.

*Cybercrime* in the *ITU National Cybersecurity/CIIP Self-Assessment Toolkit*[23], the *ITU Toolkit for Model Cybercrime Legislation*[24] aims to provide countries with model legislation that can assist in the establishment of a legislative framework to deter cybercrime.

## *Capacity Building for Policy Stakeholders*

Laws and regulations in cybercrime need to be supplemented with capacity building efforts for those charged with enforcement – regulators, law enforcement, and the judiciary. This is especially necessary in developing economies, where the police force may have personnel who are still unfamiliar with basic computer skills, let alone advanced systems and the necessary network forensic proficiencies required to investigate cybercrime and botnet cases. Additional high-level information briefings may be necessary in order to brief lawmakers and officials from relevant ministries charged with drafting and the adoption of relevant cybercrime legislation.

Besides capacity building and familiarization with computer crime and prosecution, regulatory agencies and law enforcement will require a specialized battery of tools and techniques that are necessary in order to investigate cybercrime, as well as skilled personnel to use these tools.

Experts in systems and network forensics, whose tasks include disassembling and analyzing viruses to tracing the source and activities of botnets, may not be easily available within the ranks of these agencies. Therefore, the agency may have to consider recruitment of such people, or at least rely on a panel of vetted external third-party experts, civilian researchers drawn from industry and/or civil society actors. These experts provide a ready pool of trained investigators, who can assist in evidence gathering for prosecutions as well as train other personnel from the agency.

[23] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
[24] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

### *Framework for Efficient Cross Border Enforcement in Cybercrime Prosecutions*

A comprehensive framework is required for international cooperation among cybercrime enforcement agencies, and for the protection of legitimate uses of ICTs.  This type of framework encompasses several components: a common and harmonized civil and criminal policy against cybercrime (keeping in mind the requirement of dual criminality, among others), an awareness of privacy and data protection laws that may exist in different jurisdictions, an awareness of appropriate points of contact for cybercrime law enforcement in other countries, etc.

Keeping in mind that data relevant to an investigation may remain in place for only a short time (or possibly, only while the attack is ongoing), a fast and efficient alert mechanism to put through urgent requests for international cooperation in an investigation will be necessary.

Several groups exist that promote international cooperation in investigation, the use of 24/7 hotlines for urgent enforcement requests, and other collaborative measures:

- The Council of Europe's Convention on Cybercrime
- The G8 Cybercrime Working Group
- Interpol Information Technology Crime Task Force

The Council of Europe organized the Octopus Interface conference on Cooperation against cybercrime at Strasbourg, on July 11 and 12, 2007, where delegates reached consensus to promote the development of a 24x7 point of contact network[25].  There are several coalitions of civil anti-spam

[25] http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_technical_cooperation/cyber/567%20IF%202007-d-sumconclusions1g%20Provisional.pdf

enforcement agencies, such as the London Action Plan (LAP)[26], that extend membership to industry and civil society actors.

Agencies in Australia, Korea and other Asia Pacific countries have formed the Seoul Melbourne Pact. International organizations such as ITU, APECTEL and OECD are also working on spam, malware, and cybersecurity initiatives from research and policy angles. Additionally, industry led coalitions such as MAAWG and APWG are willing to work with stakeholders from regulatory and law enforcement backgrounds.

Economies implementing cybercrime regulation and enforcement mechanisms can consider engaging with one or more of these groupings and conventions. Some of the groupings mentioned above are actively concentrating on forging links between each other and increasing cooperation in their activities, so that in the long term there is a definite trend towards consolidation of effort and collocation of meetings so that travel budget and time constraints involved in participation in a multitude of such initiatives are significantly reduced.

## *Conflicts between Cybercrime and Privacy legislation*

Privacy laws and "secrecy of communications" statutes in some countries may be stringent enough to inhibit active monitoring of their own network, and ISPs would then have to rely on external reports in order to detect and mitigate abusive traffic originating from their network, while international best practices advocate that ISPs carry out proactive and automated monitoring.

The European Commission's Article 29 Data Protection Working Party has ruled that IP addresses are personal data[27], and this means it is not easy to share such data across ISPs or CERT communities. Example #15 on page 16 of the report anticipates that "means likely reasonably to be used to

[26] http://www.londonactionplan.net
[27] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

identify the persons will be available e.g. through the courts appealed to (otherwise the collection of the information makes no sense)."

Activist privacy litigation such as the Holger Voss[28] case in Germany has resulted in ISPs prohibited from retaining IP access and other logs for other than very short periods of time, and only for billing purposes. Indeed, ISPs may not retain such logs at all, for customers on flat rate billing plans. Additionally, the ISP must delete records pertaining to a customer, on the customer's demand. Several German privacy groups have made available model demand letters[29] for this purpose.

Industries with a worldwide presence face the challenge of having a harmonized IT security and monitoring policy across their subsidiaries in economies that may have widely different laws and regulations on privacy and data protection, while at the same time ensuring compliance with local laws on this subject.

Google's Global Privacy Counsel Peter Fleischer has posted an article[30] on his blog, detailing a nuanced approach to this question, and suggesting five factors, quoted below, that an organization can use to determine whether a particular piece of information is personal data.

- How that data could be matched with publicly available information, analyzing the statistical chances of identification in doing so

- The chances of the information being disclosed and being matched with other data likely held by a third party

[28] The ruling of the District Court of Darmstadt on IP logging is available at : http://www.olnhausen.com/law/olg/lgda-verbindungsdaten.html and news reportage of this case is at http://www.heise.de/english/newsticker/news/85641/

[29] A set of model complaint letters addressed to various German ISPs and demanding deletion of a user's logs is available at http://www.daten-speicherung.de/index.php/datenspeicherung/musterklage-ip-speicherung/

[30] http://peterfleischer.blogspot.com/2007/02/are-ip-addresses-personal-data.html

- The likelihood that ‘identifying’ information may come into their hands in future, perhaps through the launch of a new service that seeks to collect additional data on individuals

- The likelihood that data matching leading to identification may be made through the intervention of a law enforcement agency

- Whether the organization has made legally binding commitments (either through contract or through their privacy notice) to not make the data identifiable

## *Framework for Local Enforcement of Cybercrime and Botnet Mitigation*

### National Framework on Cybersecurity

Mitigation of botnets, and the larger issue of Cybersecurity in general, requires extensive cooperation at national levels between different actors. In that regard, the ITU Telecommunication Development Sector (ITU-D) Study Group 1, Question 22 is developing a *Report on Best Practices for a National Approach to Cybersecurity* defining a *Framework for Organizing a National Approach to Cybersecurity*. This framework identifies five key elements of a national effort:

1. Developing a national cybersecurity strategy
2. Establishing national government - industry collaboration
3. Creating a national incident management capability
4. Deterring cybercrime
5. Promoting a national culture of cybersecurity.

This toolkit broadly follows the *Framework for a National Approach on Cybersecurity*, with aspects of the toolkit specifically targeted at botnets and their mitigation.

### Development of Nationwide Watch, Warning and Incident Response Systems

Damage and loss caused by botnets begins within seconds, or at most minutes of the botnet’s creation. The worst effects of a botnet (such as data loss, theft, etc.) typically manifest themselves within the first 24 hours. Early detection and mitigation, as well as takedown of infected hosts and C&C nodes, on a real-time basis become critical.

Takedown requires quick and efficient identification of and notification to the appropriate contact at the ISP or network to which the infected host belongs. Given the diversity of potential points of contact, it would seem expedient to identify a single organization as the nodal point of contact for botnet issues at a country level.

A proposed model for this system would be the Australian Internet Security Initiative (AISI), a Watch, Warning and Incident Response System set up as a public-private partnership between the Australian Communications and Media Authority (ACMA) who acts as the nodal agency for Australia, in collaboration with twenty-five participating Australian ISPs.

ACMA collects data about IP addresses emitting malware, and generates regular summary emails for participating ISPs, giving them details of IP addresses on their network that are infected and/or emitting malware and other abusive traffic. In the AISI framework, the participating ISPs undertake to mitigate the abusive activity originating from their IP space by individually contacting customers, modifying their filters and/or security policies, and other means.

ACMA has developed AISI as a model that can be extended to and adopted by international partners. This will be implemented in the form of a proposed strategic partnership between ITU and ACMA, so that the AISI model of a nodal agency and public-private partnerships can be extended to ITU Member States.

A similar initiative, “Operation Bot Roast”[31], has been launched by the US Federal Bureau of Investigation in cooperation with industry and civil society partners including the Botnet Task Force, Microsoft and the CERT Coordination Center at Carnegie Mellon University. Closely associated with this initiative is action taken by the FBI to prosecute several individuals engaged in botnet related cybercrime[32].

The identity, scope and mandate of a nationwide nodal agency will vary from country to country, depending on policy mandate, availability of expertise and other relevant factors.

Such an agency can be a group affiliated to the relevant ministry or agency (such as a regulator, CSIRT, or other organization) charged with cybersecurity management, and with the appropriate points of contact and in-house capacity to deal with issues.

In other countries, a national center of excellence and expertise, such as a university, may be commissioned to create a clearinghouse of information and serve as a neutral, expert third party to coordinate between stakeholders. In such cases, an appropriate government agency with a relevant policy enforcement mandate would work in close association with the national center of excellence.

Of course, contact can be established directly with the concerned ISP or the network that controls the infected IP address, if the reporting entity knows an appropriate point of contact, and the nodal agency for that country can be sent a copy of the report for their information and action.

The nodal agency uses collected reports and information gathered from other sources (either developed in-house or shared by international security research organizations) as discussed in the subsequent section on technical measures – the nodal agency thus serves as a centralized, nationwide clearinghouse for this type of information.

[31] http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm
[32] http://www.fbi.gov/page2/june07/botnet061307.htm

Information gathered by the nodal agency is analyzed to identify traces of botnet and malware activity and gather information and metrics about such activity. The nodal agency then alerts participating ISPs of attacks from their IP space, by sending periodic automated reports as well as by other procedures (including escalation points of contact).

The nodal agency additionally maintains similar escalation points of contact at the country's ccTLD registrar, and at other ICANN accredited registries within the country, for the purpose of quick notification and take down of domains registered by botherders and spammers. Given the globally distributed nature of a botnet, a domain name often serves as the single point of failure where a botnet can be taken down, or spam campaigns based on botnet activity nullified.

Given the wide variety of possible contacts, it would be advisable for the nodal agency to maintain a directory of the appropriate points of contact to report botnet activities to ISPs and other networks within their country. This list should be shared on a need to know basis. The actual names, titles and point of contact emails that ISPs mandate can be shared in this point of contact database, or a closed and secured mail and communications system may be maintained for participating ISPs and industry/civil society members.

Additionally, the nodal agency would facilitate the establishment of local (city and provincial) public-private partnerships between local government, industry, and civil society stakeholders; such partnerships would emphasize information sharing and mutual capacity building initiatives besides building up the points of contact database.

This system of a point of contacts database and regional/local partnership groups is proposed in the lines of the NCFTA[33] and Infragard[34], two law enforcement and industry public-private partnerships between the United

[33] http://www.ncfta.net
[34] http://www.infragard.net

States Federal Bureau of Investigation (FBI) and various industry as well as independent anti-spam/cybersecurity technologists. NCFTA and Infragard facilitate discreet sharing of confidential information about cyber incidents, as well as advanced training in cybersecurity investigation and promotion of security awareness, with Infragard focused on the protection of critical infrastructures.

The nodal point of contact would be introduced to some trusted organizations that are part of the security and anti-botnet/spam/cybercrime research community, drawn from government, industry, civil society, and other stakeholder groups.

Reports from these groups are trusted, and prioritized as far as is consistent with operational feasibility. Trusted reporting entities are allowed access to the database of direct ISP contacts. A non-exhaustive list of such trusted reporters may include:

- Nodal points of contact, government agencies, etc. from other countries
- CERT/CSIRT organizations
- Members of groups such as LAP, FIRST, MAAWG and CAUCE/APCAUCE
- International organizations such as APEC-TEL, APT and OECD
- Manufacturers of anti-spam and antivirus software and appliances
- Security researchers and research organizations (Castlecops, SANS, Team Cymru)
- Phish tracking and repository sites such as Netcraft and Phishtank
- Trusted block lists such as Spamhaus and CBL

Given the potentially very high volume of compromised IPs on an ISP's network, it is strongly recommended that notification of botnet/infected hosts be heavily automated, and that reports and alerts be generated and delivered in a standard, machine parseable format.

Additionally, as IP address assignments are quite often temporary and transient, with dynamic IP addressing being widely used to provide IP addresses for customer dialup and broadband access, it is recommended that such reports provide accurate timestamps showing the time when the incident occurred. Further, stakeholders in this effort are encouraged to keep their server, router and other device clocks synchronized using the Network Time Protocol[35].

Furthermore, existing and widely adopted standardized systems that are routinely used in the anti-spam and security communities for information sharing and incident response may also be deployed.

Spam reports are available from several large email providers such as AOL, Yahoo, Outblaze and others in the industry standard “ARF” (Abuse Reporting Format)[36], which lends itself to easy classification and parsing using scripts and automated incident response systems. Similarly, CERT groups have considered a standard incident handling format called IODEF[37], used to report incidents of other, non-spam, network abuse and security vulnerabilities.

### *Watch, Warning and Incident Response in a Broader Context*

Mitigation of botnets is best attempted at the network level, by involved ISPs (as discussed in the subsequent technical section). The nodal agency should adopt a model that encourages ISPs to follow best practices on network security and management. The agency itself should ideally focus on broader and more macro level issues.

In the watch, warning and incident response category, some suggested activities include:

[35] http://support.ntp.org/bin/view/Main/WebHome
[36] http://www.mipassoc.org/arf/
[37] http://xml.coverpages.org/iodef.html

- Information gathering on trends and techniques in botnet activity
- Generating and sharing metrics on malware and botnet activity
- Sharing automated alerts and other trends and analysis of information received
- Facilitating contacts between local and international stakeholders
- Deploying standardized incident response systems and capacity building in their use

Escalation points of contact will be identified at participating stakeholders for emergency handling of issues and day-to-day sharing of information that need not necessarily be in the form of automated alerts about compromised hosts.   This network of escalation points of contact can resolve issues such as the quick takedown and/or forensic analysis of command and control center hosts, domains registered by abusers under the local ccTLD.

The network can also be used to facilitate emergency closure – such as by port blocking or applying network wide fixes - of critical vulnerabilities such as zero day exploit malware.  They also serve to mitigate widespread worm epidemics such as the SQL Slammer or Storm Worm outbreaks.  Severe botnet activity targeted at a particular source (such as critical infrastructure), can also be detected and contained through a network of escalation points of contact.

### ISP Disincentives Against Individual Notification and Walled Gardens

There are several technical, financial, legal and customer satisfaction related disincentives that may be raised by an ISP, which would need to be addressed prior to deployment of systems such as walled gardens, which proactively filter spam and network abuse originating from their IP space – as well as technical feasibility reasons that deprecate against individual notification of users.

Opposition from business departments can easily kill off any proposals for increased security and user notification that are raised by the ISP's network security and anti-spam departments.  Indeed, there is a tendency among ISP business development departments to view anti-spam and network security departments as a cost center, a source of revenue loss due to users quarantined for virus infections, or terminated due to spam and other network abuse.

ISP legal departments often interpret common carrier and privacy regulations in their country as raising liability issues if they monitor their customers for abuse and filter abusive traffic, considering it conservative and risk averse for the ISP to avoid such activities.  Additionally, ISP managements may find it financially expedient to shelve any proposals for filtering and quarantine of users, and eliminate the increased capital and operating costs that result from such measures.

### Recidivism (Recurrence of Infection in Previously Cleaned PCs)

The Internet Architecture Board, during a workshop on “Unwanted Traffic”[38], has pointed out that per user notification is a costly and time-consuming exercise, but technically of limited utility in actual mitigation of botnets due to the high risk of recidivism – the chance that a cleaned up PC will get re-infected.  Notifications from the ISP have limited impact on end user repair behavior.

The following are some typical user responses to such a notification: Among other things, users may:

- Ignore it as just an ordinary virus infection.
- Possibly clean their PC
  - Only to have it re-infected by another virus within the next few days
- Simply buy a new PC, which may have the same set of vulnerabilities as their old PC

[38] This section is adapted from a workshop on “Unwanted Internet Traffic” held by the IETF's Internet Architecture Board. The workshop's proceedings are summarized in RFC 4948 - http://www.isi.edu/in-notes/rfc4948.txt

- If pirated software is installed onto the new PC, it is insecure from the beginning

Further, the infected PCs, old or new, with or without updates, are used by the same users with the same behavioral patterns, and it remains entirely possible, and far too common, for a user to be tempted by the offer of, say, a free screensaver, into overriding all the existing protection and warnings that his antivirus software generates.

Many infections are quite hard to remove, as they may disable windows update, as well as block access to the websites and update servers of Antivirus and Security software vendors. This  is achieved by the malware modifying the “hosts” file on the PC to point update servers to entirely different IP addresses, changing the configured DNS settings to point to spammer controlled name servers that return bogus answers to DNS queries, or even replacing the software libraries that Windows uses to do DNS lookups.

Attempting to clean up the infected PC by downloading the latest security updates from Windows/ various antivirus vendors may result in further malware downloaded onto the PC from a spammer controlled update server. This strategy is also used to redirect the user to a phishing site when he tries online banking or e-commerce website. Another common scenario is that adults in a home would be careful in their use of the family PC, keeping it secure and using it for their e-banking and other transactions.  However, all this care is overridden because their children may use the PC to download what they think is a screensaver, instead installing a trojan that steals bank information.

Empirical observation shows that there is no significant difference in terms of repair behavior between different industries or between business and home users.  Users' patching behavior follows an exponential decay pattern with a time constant of about 40 percent per month[39]. Thus, about 40 percent of computers tend to be patched as soon as an update is released, and approximately 40 percent of the remaining vulnerable computers in each following month will show signs of being updated. This leaves a few percent still not updated after 6 months. This effectively translates to millions of computers connected to the Internet that will remain vulnerable to infection for the rest of their life.

### Financial Disincentives to the Deployment of Walled Gardens

Walled Gardens have now become critical to the operation of an ISP oriented watch, warning and incident response system. However, the implementation of walled gardens is a technically complex and expensive process and may involve the deployment of expensive new equipment and modifications to the existing network structure.

ISPs offering internet access as a commodity in a price sensitive market focus on driving down capital and operating costs, in order to provide broadband at a cheaper rate than the competition. Therefore, they may operate with minimal levels of staffing and service to lower operating costs.

There is a high initial capital expenditure in installing firewall and other equipment to detect and quarantine infected IP addresses, and to provide mechanisms to remove users from quarantine. There is a further high operating cost for supporting users quarantined in “walled gardens” or deactivated for emitting malware/spam.

### Customer Dissatisfaction Issues Due to Notification and Walled Gardens

Besides the financial disincentives related to the quarantine, filtering or notification of users, several ISP business departments perceive such efforts as causing an inconvenience to their customers, resulting in the ISP facing brand damage and customer dissatisfaction.

[39] This is the “40-40-20” rule proposed by Sean Donelan, http://www.donelan.com

Users faced with quarantine or account termination are likely to complain at multiple levels, leading to increased load on support and call center staff, and a certain amount of customer dissatisfaction.   Using a call center to notify a customer in response to an AISI or walled garden alert and to receive calls from customers complaining about being warned or deactivated can be quite expensive.

ISPs in developed countries may face an average cost of over USD 15 per call made or received by the help desk, with several calls made every day due to the high number of infected users.   Sending emailed notifications will reduce the cost of outgoing phone calls, but does nothing to reduce the cost of staffing a helpdesk.  Further, irate users may call their ISP and demand that they “talk to a human being” rather than receive boilerplate emails.

These costs may well be cheaper for developing economy ISPs, and can become cheaper for ISPs in developed countries if they outsource their call centers to a cheaper location, but these costs will remain significantly high, and there will be several such calls made every day.  ISPs can act to reduce call volumes by providing “quick release” mechanisms that automatically remove quarantines after a short period, and allow the user to click a button on the ISP's support page in order to indicate that the user has disinfected his/her PC – releasing his/her IP address from the quarantine.

### Advantages of an ISP Deployed Watch, Warning and Incident Response System

As noted in the previous section, ISPs face strong financial, business and policy disincentives when deciding to operate their own watch, warning and incident response systems.  Yet, these are essential to facilitate near real time detection and mitigation of network abuse and malicious traffic.

Staffing issues and time constraints make it imperative that the nodal agency and participating stakeholders automate the reporting and take down of spamming users, or individual compromised PCs that are merely nodes in a botnet, remote-controlled to emit spam or launch DDoS attacks.  It is imperative that incident response be backed by network level mitigation of malware and botnet activity, as discussed in the subsequent section on technical measures.

The notification process is highly useful and essential since these notifications serve as a channel to alert the public to specific issues.  The agencies and participating ISP's efforts to reach out to end users and victims of botnet activity are part of a broader awareness campaign and will help to generate word of mouth publicity and increased awareness of botnets.

The sheer cost of such notifications, especially if such notifications are from a government agency, will motivate ISPs to improve network level security and follow other industry best practices for abuse mitigation, as detailed later in this article.  For several developing economy ISPs, such security ensures that bandwidth, a scarce and costly resource for several countries, is saved from being wasted by spam and malware.

ISPs risk being blocked by other ISPs due to emission of abusive traffic from their IP space, leading to falling customer confidence due to customers not being able to email various ISPs, or access popular websites, due to the remote ISP or website having blocked the ISP's IP ranges.

There is a further loss of reputation from being named in the “Top 10 Spam Source” lists published by vendors of anti-spam and antivirus products, which receive widespread media coverage and are regularly cited in articles on spam, malware and botnets.  Avoidance of such negative publicity may motivate ISPs to act in cases where economic considerations deprecate any increase in filtering.

Alerts channeled to the ISP by a watch, warning and incident response system operated by a government agency, and possibly clarification of privacy and common carrier laws to provide a safe harbor for ISPs making Good Samaritan efforts to filter spam and malicious traffic originating or entering their network, might help influence decision makers weighing the deployment of filtering.

US Code 47 USC 230 (c) (2)[40] provides an example safe harbor provision. A recent United States district court decision in Zango v Kaspersky Lab, Inc[41] illustrates the application of this code in a case where an Adware vendor sued a vendor of security software for listing their product as spyware. The case was dismissed in favor of the security software vendor Kaspersky Inc.

A discussion[42] of the incentives an ISP actually has to consider when implementing walled gardens, is available on the Arbor Networks security blog ASERT[43].

This article states that botnet-related activity, especially when reported to an ISP as part of a sustained nationwide campaign against botnets (such as the FBI Bot Roast), would highlight the accumulating impact of each infected PC on the ISP’s network, on their ARPU (Average Revenue Per User) and subscriber churn – a so-called “Death by a Thousand Duck Bites”.

The conclusion reached in the article is that implementing automated botnet mitigation mechanisms and working to reduce the amount of botnet activity on an ISP’s network actually helps, in the long run, to improve ARPU and lower subscriber churn at the ISP.

[40] http://www4.law.cornell.edu/uscode/html/uscode47/usc_sec_47_00000230----000-.html
[41] http://www.circleid.com/posts/791111_zango_verdict_spam_filters_blacklists/
[42] http://asert.arbornetworks.com/2007/09/isp-death-by-a-thousand-duck-bites/
[43] http://asert.arbor.net

# Annex B – Technical

## *ISP Best Practices to Mitigate Botnet and Malware Activity*

ISPs providing Internet and email, as well as other messaging services (such as instant messaging (IM), chat etc) access to users can take several steps, widely regarded as industry best practices, to filter out or otherwise mitigate botnet and malware activity.  This is required to protect their users and their network from such activity and to prevent the emission of such activity from their network (from infected PCs, or actual network abusers who may be on their network).

Organizations such as MAAWG[44] and the IETF[45] and IAB are working on best current practices in this area.  These processes are open and participative.  ISPs and other interested stakeholders in developing economies would be encouraged to participate, and to track these by active participation in security and anti-spam related mailing lists, even if actual participation in physical, face to face group meetings may not always be feasible due to budget and other issues.

These include the following technical measures, as well as active participation in other measures discussed elsewhere in this paper, and which straddle all three categories (policy, technical and social measures) and must be integrated into a broad based security strategy.

### Filtering of Inbound Email to ISP users

The need for inbound filtering, to protect networks, and to protect users on the network, from external threat sources (spam, DDoS, malware etc) has

[44] http://www.maawg.org/about/publishedDocuments/ ITU is working with MAAWG to release a set of MAAWG best practice documents, translated into the UN official languages.
[45] http://www.ietf.org/html.charters/opsec-charter.html

been widely recognized and there is a multitude of vendor solutions and best practice documents covering this aspect of filtering.

Filtering methods, at a basic level, involve the use of locally compiled as well as publicly available IP block lists such as those provided by The Spamhaus Project[46], and URL block lists such as SURBL[47], in addition to methods such as HELO filtering, Graylisting and Banner Delay. Additionally, ISPs may install antivirus filtering, to filter out malware from their user's mailboxes.

### Outbound Filtering

Besides Inbound filtering, ISPs and network operators have begun to develop consensus that that they should attempt to contain abusive traffic originating on their own network, before it leaves their network and becomes a problem for other ISPs. Several best practices exist, documenting various forms of "outbound" or "egress" filtering on routers, as well as filtering techniques implemented on ISP outbound mail servers that handle email traffic originating from an ISP's users.

### Router Level Filtering, Including Filtering of Spoofed Source Address Traffic

Some malicious traffic tries to spoof the source IP address, and it is a widely recognized best practice to filter out packets from spoofed source addresses[48], as well as from unallocated or unroutable networks (so-called "bogon"[49] or "martian" traffic). The UK government's Center for the Protection of National Infrastructure has made available in 2004 a set of best practices[50] on BGP (Border Gateway Protocol) router level filtering.

A broader and more up to date overview of router level filtering best practices is available in presentations by Upadhaya[51] and Matsuzaki[52].

[46] http://www.spamhaus.org/zen/
[47] http://www.surbl.org
[48] http://www.faqs.org/rfcs/rfc2827.html
[49] http://bogons.cymru.com
[50] http://www.cpni.gov.uk/Docs/re-20040401-00392.pdf
[51] http://www.apnic.net/meetings/22/docs/tut-routing-pres-bgp-bcp.pdf

Presentations used in several “tutorials” and “bootcamps” focused on ISP security are available for download on the Cisco FTP site[53]. There are several textbooks published by router vendors and technical publishers, which include detailed technical measures that ISPs can implement in order to improve network and router level security.

The NSP-SEC[54] community is a vetted volunteer community of security operations personnel from various network service providers, focused on incident response, which coordinates the interaction between network service providers around the world in near real-time. The NSP-SEC community tracks exploits and compromised systems and mitigates the effects of these on ISP networks.

### Management of Port 25

MAAWG[55] recommends the following set of Email Transmission Best Practices for Internet and Email Service Providers, that are widely deployed by MAAWG member ISPs, as well as other ISPs around the world, with, in MAAWG’s opinion, no appreciable decline in customer base. The MAAWG Best Practice document on “Managing Port 25” states that ISPs must:

- Provide Email Submission services on port 587, as described in RFC 2476.
- Require authentication for Email Submission, as described in RFC 2554.
- Abstain from interfering with connectivity to port 587.
- Configure email client software to use port 587 and authentication for Email Submission.

[52] http://www.apricot2007.net/presentation/conference/security_stream/anti-ip-spoofing.pdf
[53] ftp://ftp-eng.cisco.com/cons/isp/security/
[54] http://www.nspsec.org
[55] http://www.maawg.org/port25/

- Block access to port 25 from all hosts on their network, other than those that are explicitly authorized to perform SMTP relay functions.
    - Such hosts will certainly include the ISP's own Email Submission servers and may also include the legitimate Email Submission servers of their responsible customers.
- Block incoming traffic to their network from port 25, other than to their mail servers. This prevents potential abuse from spammers using asymmetric routing and IP spoofing.

A detailed treatment of these best practices is available in draft Best Current Practice RFC by Hutzler[56] et al. Providers of all sizes, including many of the most popular service providers in the world and many MAAWG members, have adopted these practices without any appreciable reduction in customer base – a common concern cited by potential adopters of increased filtering and notification mechanisms.

### Authentication Mechanisms

Going beyond basic filtering techniques, ISPs may verify incoming email based on various authentication mechanisms[57], such as DKIM, Sender ID and SPF, which sending domains publish in order to verify the authenticity of email purporting to be from their domain. Additionally, ISPs checking such authentication mechanisms would be encouraged to deploy sender authentication to help other ISPs verify outbound email sent by their users.

Sender Authentication mechanisms such as Sender ID and SPF are based on the principle of "path authentication", where a domain's administrator publishes a TXT (text) DNS record in a standard form, to declare a list of valid servers that a domain will emit email from. In an alternate approach called "message authentication", domains can sign email using a set of

[56] https://datatracker.ietf.org/idtracker/draft-hutzler-spamops/

[57] Overviews of these mechanisms are available at DKIM: http://www.dkim.org, at SPF: http://www.openspf.org and at Sender ID: http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx

lightweight cryptographic keys, based on the email's content, and its headers, which mail servers insert to show mail path and routing information when email is sent or received.

The difference between these approaches is that path authentication asserts that the email came from a valid server that is authorized to send outgoing email for the domain, while message authentication asserts that the message is valid, independent of the actual servers it passed through.

### Issues with Path Authentication Mechanisms (Sender ID and SPF)

Path Authentication mechanisms are trivial to deploy and do not require any additional resources, as TXT records are a standard feature of DNS and all major DNS software supports TXT records.  These records are, therefore, the least resource intensive method to validate the origin of an email. However, the major Path Authentication mechanisms, Sender ID and SPF, have gone through several iterations of development, and dogged by vociferous debates and controversy[58] based on technical and ideological viewpoints, so there are now several variants of SPF deployed, which differ in minor but significant ways.

It may be quite hard for a domain's administrator to compile a complete, authoritative list of all the sources which may originate email with a "from" address in the domain.  For example, a large nationwide ISP or email service provider may have several mail servers spread across multiple networks.  A corporation may have external contractors or vendors authorized to send email with a from address in the corporation's domain, but such emails may well originate through a different set of mail servers, not under the corporation's control.

Path Authentication has issues with the handling of forwarded email, where email received for a user forwards to another of the user's email address,

[58] An overview of the controversies and issues surrounding SPF, by noted antispam researcher and mailserver developer John Levine is available at: http://www.circleid.com/posts/spf_loses_mindshare/

which may be on a different server. Another common issue with Path Authentication is noticeable cases where users use an alternate SMTP server (such as a hotel mail server) when they are traveling.

In both cases, as well as where an administrator may not be aware of all possible sources of email for the domain, valid email may be inappropriately rejected if the domain publishes a path authentication mechanism such as SPF or Sender ID without taking precautions[59] to account for offsite or forwarded users' mailboxes.

### A Conservative Approach to the Use of Authentication Mechanisms

ISPs filtering email based on authentication mechanisms may, if feasible, wish to deploy these as part of a "scoring system". A scoring system is a set of filters that assigns a weighted probability of spam to incoming email, so that several different characteristics of an email's source, routing and content are taken into account in order to decide whether a particular piece of email is spam or "ham" (non spam). Based on the probability that an email is spam, the ISP may elect to reject the email, route it to the user's spam folder, or deliver it to the user's inbox.

### Issues with Message Authentication Mechanisms (DKIM)

Message Authentication Mechanisms validate the actual message rather than attempting to validate the path, and therefore avoid issues concerning forwarded email and offsite users. However, DKIM is comparatively more difficult and resource intensive for an ISP or email provider to publish, as it involves signing each message with a cryptographic hash.

Validation of email also involves validation of these cryptographic signatures, which is again quite resource intensive. Publication and verification of DKIM signatures may therefore require ISPs to deploy more

[59] Besides publishing a comprehensive and authoritative list of mailservers that are valid sources of email for a domain, the domain administrator may consider publication of "loose" records such as ~all and ?all. These loose records declare that email for a domain may originate from sources other than those mentioned in the SPF or Sender ID record, and the rewriting of the smtp MAIL FROM: for forwarded email using the SRS mechanism.

hardware resources for their email infrastructure, so that the costs involved in implementing this may also become a consideration for some ISPs.

### Reputation Systems to Complement Authentication

The concept of authentication, whether path based or message based, serves to declare that an email that claims to originate from a particular domain indeed did originate from that domain.  However, this information is not complete without considering another factor – the reputation of the domain, whether it is spam or not spam.

An analogy would be that while a movie theater's marquee, and the movie ticket, may both declare that a particular movie is being screened (authentication), both these facts tell us nothing about whether the movie is a good one or not (reputation).  In addition, it is entirely possible for different people to have different opinions about the same movie.

This is an illustration of the fact that the just as the reputation of a movie may vary from person to person, the reputation of a particular domain might well be different at different recipient domains.  An email marketing firm might be regarded as responsible and reputable by one ISP, while a different ISP may have serious issues with the same marketer, and block all email from them.

In the context of this document, it is quite common for spammers and phishers to publish valid authentication records for their domains, hoping to increase "deliverability" (the acceptance rate of their email by ISPs) by this step.

Besides locally maintained blocklists and whitelists that ISPs maintain as part of their filtering strategy, which can be considered negative and positive reputations, as well as public blocklists (again, negative reputation services), there are a variety of firms emerging that provide broader reputation services, to complement the deployment and use of authentication.   These providers audit a company's email practices and certify that their practices meet a certain set of standards that are broadly acceptable to ISP anti-spam teams and recognized as best practices for email marketing.

## *Technical Components of a Watch, Warning and Incident Response System*

### System and Network Forensics Toolkits

Evidence gathering on matters of cybercrime quite often requires a detailed examination of a compromised and infected PC's software internals, such as lists of modified files and registry entries and forensically intact copies of the malware. Investigators also need to collect detailed information on the activities carried out by the malware once an infected PC is connected to the Internet. Such activities include making connections to a command and control server to receive instructions, the local installation of a phishing or other illegal website on the compromised PC, participation in password cracking attempts and DDoS attacks, or other botnet related activities.

Several law enforcement organizations investigating cybercrime, as well as other online abuse issues such as child exploitation, tend to use specialist forensic analysis software for this purpose. They additionally employ customized “live CDs” (often running a version of Linux). This “live CD” provides a complete operating system installed with forensics tools that can be temporarily loaded on to an infected PC simply by inserting the CD into a drive and rebooting the PC. This leaves the infected PC and its contents intact, while allowing the examination of the PC and isolation of any malware or other illegal content on it.

Infrastructure that can be used by the nodal agency to store and collate reports for the purpose of enforcement actions is available, among others, from vendors such as SpamMatters, which provides the Australian Communications and Media Authority with a spam reporting and analysis system for enforcement of the Australian Spam Act of 2003.

Additionally, ENISA, the European Network and Information Security Agency, links to several resources[60] that can be used by CSIRT and CERT teams for incident response and handling.

### Identification of IP Space Controlled by an ISP: Whois and Rwhois Records

Alerts or escalations generated by the nodal agency, or by other stakeholders who contact the ISP directly to report an issue, can be keyed to public databases of IP assignment and routing, such as ASN (Autonomous System Number) and IP whois databases maintained by the RIRs (Regional Internet Registries[61]).

However, several ISPs, especially in developing economies, may not always accurately update ASN and whois information to reflect the current state of IP allocation within their network.  Larger “tier 1” ISPs may also sub-allocate smaller blocks of IP space to customer ISPs or other networks without simultaneously updating whois information.  In such a case, querying whois may show large swathes of IP space owned by a larger ISP, while the actual ISP using the relevant IP number may actually be a customer, or a customer of a customer, of the larger ISP.

In such complex cases, a short term solution would be for the nodal agency to maintain a local database of IP space operated by participating ISPs, to be updated as and when the ISP acquires new IP space or relinquishes old IP space (for example when assigned a new IP block when switching between upstream connectivity providers).

This model is, however, time consuming and there is a quite high potential for stale data, where an ISP changes its actual IP space but the nodal agency's IP database is not updated accordingly, so that alerts or escalations may end up being sent to the wrong person or organization.  A more

[60] http://www.enisa.europa.eu/ENISA%20CERT/pages/04_02.htm

[61] RIRs are the bodies responsible for IP address allocation in a particular region, such as ARIN for North America, RIPE for Europe, APNIC for the Asia Pacific region, AFRINIC for Africa and LACNIC for Latin America.

effective and long term solution to this issue is to encourage participating ISPs to maintain clear and accurate IP and domain whois records at their registrar and at the relevant Regional Internet Registry.  There are, of course, cases involving smaller allocations of IP space (such as allocations of less than a /24, or 256 IP addresses) that a large ISP may allocate to its smaller customers, and for which the ISP may not wish to update IP whois records.

In such cases, the ISP that controls the larger IP block may elect to accept alerts for these smaller customer IP blocks and pass them on to the appropriate points of contact within the customer.  ISPs may also operate a “rwhois” server that will reflect assignments of such smaller blocks of IP space - such information is also available for contacting the IP's network administrator directly instead of going through the ISP.

### Automated Detection and Reporting of Botnet Hosts

The nodal agency, and participating ISPs, can gather information on malware and botnet activity by several active and passive measures, including but not limited to those outlined below in this paper.  The gathered data is used to gather information for the purpose of enforcement actions and prosecutions, compile metrics and provide a source of automated alerts for participating ISPs.

Input from all these measures below is used to feed into a national Watch, Warning and Incident Response system, on the lines of the Australian AISI.

### Real Time Feeds of DNS Block Lists that Target Malware Activity

The Spamhaus XBL[62] blocklist of exploited hosts is a huge database of compromised IP addresses that is updated several times a day and contains thousands of such IP addresses, compiled by integrating together several such blocklists that publish lists of compromised hosts, including the largest such blocklist, the CBL[63].

[62] http://www.spamhaus.org/xbl/
[63] http://cbl.abuseat.org

A complete copy of the XBL can be fetched on a regular, automated basis by the nodal agency, fed into the AISI system that they operate, and used to channel reports to participating ISPs whose IP address(es) are listed in the XBL due to their being detected emitting malicious traffic.

Besides the Spamhaus XBL, the AISI instance can accept other feeds that may be made available from various private and public sources, as well as malicious traffic detected by some of the measures described below, that will be deployed in countries implementing this toolkit.

### Honeypot Systems

Honeypots work in much the same way as a real pot of honey works to attract flies – but these “honeypots”, deployed on the Internet, attract spam and malware emails, rather than insects.  Such honeypots are dedicated “spam trap” domains, set up solely to collect spam and malware.  They have no actual users.  Huge lists of email addresses are created on these domains, seeded in public places such as fake websites, which though publicly accessible on the Internet, have no actual content except long lists of these email addresses.

Honeypots are quite simply traps baited for “harvesters”, bots operated by spammers that crawl the Internet looking for email addresses, and adding these to databases of email addresses which are then used to send out spam, or sold to other spammers, as well as to legitimate but gullible email marketers, as “millions CDs”.  These are CDs advertised as containing millions of email addresses that have “opted in” to receiving marketing solicitations by email.  Any email received at a Honeypot or Spamtrap address is, by definition, unsolicited and spam.

Other honeypots, that are focused on tracking botnets and malware will deliberately infect a computer with viruses, spyware or other malware and operate it inside a “sandbox”.  All incoming or outgoing network traffic from the PC is logged, monitored and subsequently analyzed to gather information on infection vectors, attack strategies, and command and control mechanisms used by the malware and its associated botnets.

Information gathered in the honeypot, in addition to the information gathered from reports from relevant stakeholders, is stored in a format that maintains forensic integrity (so that the information can be used as evidence in prosecutions), and analyzed to gather information that may be used to:

- Update spam and malware filtering systems on a near real-time basis (automated updates to filtering can happen within a very short time of the spam or malware being collected)
- Identify spam, malware, and botnet activity that has a country link, in order to gather evidence for potential enforcement actions and prosecution under the country's anti-spam and cybercrime laws.
- Identify trends and compile metrics on spam, botnet and malware activity.

Infrastructure for the setup of spam trap honeypots is available from groups such as Project Honeypot[64]. Project Honeypot provides software for installation on websites, so that any bot that visits the website for the purpose of harvesting and spamming email addresses will end up collecting some of these spam trap addresses. Data gathered from Project Honeypot is used by the project to launch litigation[65] against spammers.

The Honeynet Project[66] provides honeypots and other resources that are used to track botnets. The Honeynet Project is part of a global Honeynet alliance[67], with member organizations from more than twenty countries joining to install honeypots and track and monitor botnet activity.

### Darknets and Flow Based Analysis

The principle behind flow based analysis of Internet traffic is quite similar to that of Sonar, operating on the observation of network traffic patterns and subsequent detection of any anomalous traffic. Traffic patterns and

[64] http://www.projecthoneypot.org/
[65] http://www.projecthoneypot.org/5days_thursday.php
[66] http://www.honeynet.org/tools/index.html
[67] http://www.honeynet.org/alliance/index.html

disruptions caused by specific anomalies can be “fingerprinted” so that any recurrence of a particular pattern can lead to rapid threat identification. Such analysis is often referred to as a “Network Telescope”. The Cooperative Association for Internet Data Analysis (CAIDA) carries out extensive flow based analysis and maintains a taxonomy[68] of analysis tools.

Darknets are a specialized kind of honeypot widely used in flow analysis. A darknet is a large netblock of assigned and routable IP space that is not bound to any particular host (an analogy would be a valid telephone number allocated to an organization, but not assigned to any particular telephone). Any activity that is observed to “originate” from such unassigned space must therefore be spoofed traffic, such as port scanning, worm / virus activity, DDoS, etc., with the malicious activity attempting to disguise its origins by claiming to be from a totally unrelated IP address (which quite frequently happens to be monitored by darknets).

The “Internet Motion Sensor”[69] is a globally scoped threat monitoring system that has sensors and darknets deployed at major ISPs, enterprises and academic networks around the world, monitoring over 17 million “prefixes” – approximately 1.2 percent of the available IPv4 address space – that is yet unallocated and that can be freed up for distribution to networks that need additional IP addresses.

As mentioned earlier in this document, spammers and botherders will actively attack and attempt to penetrate or take down honeypots, darknets as well as the websites and other infrastructure of organizations known to be engaged in research, scanning, detection or take down of botnets. Given the criminal connections that spammers and botherders have, there may also be a threat of actual physical harm to personnel engaged in such research. Adequate physical and network security precautions need to be taken, and

[68] http://www.caida.org/tools/taxonomy/index.xml

[69] http://ims.eecs.umich.edu/

data generated by such research needs to be shared on a need to know basis, and anonymized as necessary.

### Collection and Analysis of Anonymized Server Log Files from Participating ISPs

Spam, intrusion or attack attempts, malware deployment, and other malicious activities inevitably leave traces of their intrusion in the system and network logs of the attack vector and target.  These traces include signs of brute-forcing passwords by trying multiple random passwords till one succeeds, attempts to install a particular malware, access to specific files and directories on hacked systems, a particular botnet command and control host, etc.

Systems and Network level forensic techniques are employed to analyze log files and compromised systems in order to investigate malware and botnet traffic (as well as spam and other Internet threats).  The collection of server log files and network flow statistics on a real time basis and their subsequent automated analysis is a potent tool to discover and mitigate attacks that are in progress, and to analyze a just completed attack, a newly released malware etc so that future recurrences of the attack can be detected and mitigated far in advance.

In order to preserve user privacy, usernames can be anonymized or otherwise encrypted, and log files analyzed by a neutral third party with no commercial or other privacy related interests in the data (such as a university research facility) under the terms of a strict NDA and privacy agreement. Alternatively, ISPs can agree on a shared set of tools and techniques to analyze such data, and share only the results and metrics gathered from their investigation, after sufficient anonymization of personally identifiable information of their users.

## Passive DNS Replication and Analysis of gTLD and ccTLD Zones[70]

Passive DNS, used by Florian Weimer[71] et al. at RUS-CERT[72], and the Security Information Exchange at ISC[73], among others, analyzes a domain's DNS setup by analyzing responses the domain's DNS servers return to specific queries. Substantial amounts of data on botnet related DNS activity is obtained from such analysis of suspect domains, with passive DNS tied to a honeypot / honeynet sensor network and to the analysis of anonymized server log files from participating ISPs.

The DNS data that is analyzed tends to be much more reliable than the data available in whois for a domain, which is likely to be outdated, or falsified by the botherder. In particular, analysis of DNS queries generated by malware infected IP addresses can lead to quick detection of botnet command and control centers, reveal other nodes in a botnet that the infected machine attempts to contact, and also to detect the malicious activities that the botnet is engaged in.

Passive DNS analysis is further backed by analysis of the root zone file of various gTLDs and ccTLDs. Most gTLDs are under contractual obligation to ICANN to publish their zone files, which are made available for download on signing a contract with the registry controlling the gTLD. A partial list of links to the various registry pages that specify zone files is given below:

- .com and .net (from Verisign): http://www.verisign.com/information-services/naming-services/com-net-registry/page_001052.html
- .org (from PIR): http://www.pir.org/RegistrarResources/ZoneFileAccess.aspx

[70] To be read in conjunction with the subsequent section from this paper, that discusses registry and registrar best practices and whois privacy

[71] http://www.enyo.de/fw/software/dnslogger/

[72] Rechenzentrum Universität Stuttgart Computer Emergency Response Team: http://cert.uni-stuttgart.de

[73] http://www.isc.org

- .biz (from Neulevel): https://www.neulevel.biz/zonefile/
- .info (from Afilias): http://www.afilias.info/faqs/for_registrars/general_registrar#e

Access to ccTLD zone files is generally not available, and detection and mitigation of botnet activity on ccTLD domains using zone file analysis will require engagement with the registry for that ccTLD, and with local cybercrime / antispam regulators and law enforcement.

Passive DNS replication can certainly be used to analyze specific ccTLD domains detected in botnet activity. It is however preferable to actively engage with registrars and registries to arrange a standard operating procedure for quick the take down of such domains and preservation of evidence for future prosecution.

Botherders tend to register hundreds or even thousands of such domains, using only a small portion of these at any given time and retaining the rest in reserve. However, analysis of the actual TLD or TLD zone file, either by trusted independent researchers who sign contracts with the registries to gain access, can identify a much larger number of malicious domains.

The registrars themselves can identify several more botnet domains when they combine data from zone file analysis with regular audits of their billing database to identify signs of fraudulent registration activity, such as the use of stolen credit cards to register a domain, or a pattern of bogus whois records. Registrars should additionally watch for such signs of fraudulent registration activity on any resellers that they authorize to sell domain registration services on their behalf.

## *ISP Organized Watch, Warning and Incident Response Systems*

### Walled Gardens

Port 25 management only serves to mitigate spam originating from botnets. As discussed earlier in this article, botnets are capable of much more than just spam, and the botnet problem does not get solved by merely managing port 25 – that is, admittedly, regarded as an essential first step best practice for ISPs.

ISPs need to explore methods to automatically detect IP addresses emitting malicious traffic, and quarantine them in order to mitigate the levels of abusive traffic originating from their network. An increasing number of ISPs in the USA and Canada, as well as other countries, are beginning to deploy walled gardens[74], in order to automatically detect and quarantine sources of abusive traffic.

The walled garden can be used to automatically isolate hosts against which alerts have been received through the AISI mechanism as implemented by the nodal agency for cybersecurity in the ISP's country, as well as other trusted sources of alerts such as CERTs and ISP feedback loops.

### Feedback Loops and Report as Spam Buttons

ISPs routinely deploy "report as spam" buttons on their webmail service, or as plug-ins to email client software such as Outlook, for their customers to report spam that they receive in their mailboxes. The report spam button ensures that the ISP gets a constant stream of spam reports in near real time, as users are quite likely to click "report spam" buttons as soon as they see spam arrive in their inboxes. These spam reports are used by the ISP to tune their filters and block spam sources on a faster, more automated basis.

ISPs can additionally set up "feedback loops" – a form of Watch, Warning and Incident Response alert system, where other ISPs, network administrators as well as senders of email marketing messages, can give the ISP a list of their IP ranges. Once a "sender" has requested a feedback loop from an ISP, any email from the sender's IP ranges that the ISP's users report as spam is forwarded to the sender for action. The reported email

[74] Please see also an earlier section in this paper on the feasibility and ISP incentives for individual alert systems

message is first anonymized by removing the recipient's personally identifiable information, before being forwarded through the feedback loop.

A standardized format called the Abuse Reporting Format (ARF)[75] has been developed by ISPs deploying feedback loops, in order to ensure the interoperability of feedback loop setups, so that a standard set of programs can be used to process feedback loops received from several ISPs. ARF formatted emails can be processed to extract data such as the sending IP address and the sender's email address, so that senders whose email generates a high complaint rate (potentially spammers) can be quickly identified. Reportage in a standardized format such as ARF ensures the forensic integrity of the email and preserves the complete headers and other components of the email so that, excepting the removal of personally identifiable information from the email, its structure and format are exactly the same as when the email was received.

ISPs may process complaint data obtained from feedback loop reports manually or automatically to identify and deal with spammers or sources of abusive traffic (such as infected PCs) on their network. Automation can combine feedback loop data with other factors such as the age or previous history of the account and this data integrates into an outbound spam control system to quickly detect and mitigate spam or abusive traffic. For example, a newly created account emitting large quantities of spam or a PC that has a history of virus infections can be deactivated much quicker than an account that shows a pattern of responsible use.

America Online[76] was the first ISP to introduce the concept of a feedback loop. Several other ISPs such as Earthlink, Hotmail, Outblaze, Roadrunner and Yahoo have also implemented such feedback loops. Some ISPs that offer feedback loops may require that publish their IP ranges in the form of a SPF or SenderID record), so that any changes to the sender's IP ranges can

[75] http://www.mipassoc.org/arf/
[76] http://postmaster.info.aol.com/fbl/

automatically update the feedback loop without the sender having to request the ISP to update their loop each time they add or remove IP ranges.

Additionally, agencies seeking reports on spammer activity can work with ISPs to deploy report spam buttons that, when clicked will send these reports in a manner that maintains the forensic integrity of the spam, so that it can be used as evidence in any prosecution or other enforcement actions. The Australian Communications and Media Authority (ACMA) has made available such a system, provided by SpamMATTERS[77], to Australian Internet users, and some Australian ISPs have also integrated the SpamMATTERS reporting tool into their webmail service.

## *Provision of Secure ICT Resources to ISP Users*

Computers and other Internet capable devices connected to an ISP network are much more vulnerable to infection and compromise when improperly secured.  These devices are even more vulnerable if they are not kept up to date with critical security updates.  Every layer of security that is added to an Internet connected device reduces the probability that it will be compromised and made part of a botnet, or otherwise hijacked and made to emit abusive traffic.

ISPs focused on mitigating botnet and malware abuse on their network, as well as reducing the cost required to deal with the quarantine or termination of infected hosts and other sources of abusive traffic on their network, must work towards increasing the security of devices on their customer network. Possible measures ISPs can take include:

- Equipping DSL routers or other CPE (Customer Premises Equipment) with a basic firewall.

[77] http://www.acma.gov.au/interforms/spam/spammatters.htm

  - The router’s management console, and the customer’s local network, must default to not being accessible over the Internet, only from within the customer’s network.
  - CPE devices often have a default username and password like “admin/admin”, and making such a router’s management console accessible over the Internet would inevitably lead to its compromise.
  - Any administration console access that an ISP may have installed on customer routers, for automated upgrade or technical support of the router, must be restricted so that only IP addresses from the ISP’s Network Operations Center (NOC) can access the console from outside the user’s home network.
  - ISPs must encrypt such maintenance channels, for additional security.

- Providing free and/or discounted firewall, antivirus and antispam software to their users.
  - Several customers may not buy an antivirus and firewall product for their PC at all, or allow their antivirus and firewall licenses to lapse, so that their computers remain unprotected. Free or cheap software will motivate users to protect their systems.
  - This software can be distributed in the “welcome pack” that ISPs routinely give new customers, or made available for download on the ISP’s website

- Setting up local clusters of the various content distribution networks such as Akamai will help provide fast, local access to the Windows Update servers, as well as those of major antivirus and security software vendors. This fast local access to updates reduces the time taken for the user to download a security update, and thus minimizes the amount of time he spends online with his computer vulnerable, until the update has been installed.

## *Registrar and Registry Best Practices on Spam and Botnet Domains*

### Fast Flux Hosting and Rock Phishing

Botnets are rapidly moving away from centralized command and control servers (such as an IRC channel) – which presented a single point of failure, to more decentralized methods. They have been moving to domains and using the DNS as a control channel, with hundreds of domains registered for a single botnet campaign. Fast flux botnets make extensive use of the robustness and resiliency of DNS to defend themselves against take down by ISPs, law enforcement (or by other botherders who prefer to hijack an existing botnet rather than to build their own). A comprehensive overview[78] of Fast Flux is available from the Honeynet Project and Research Alliance.

With a typical domain, the hostnames and IP addresses associated with the domain do not change often, if at all – most domains continue for years with a set of standard hostnames like mail.domain.com and www.domain.com, associated to specific IP addresses that may change only when the domain name moves to a different ISP or hosting provider.

Fast-flux DNS on the other hand uses a large number of domains and "servers" - in fact, every host in a botnet becomes a potential fast flux server. Domain names used for botnets rapidly cycle between domains, and within a domain, the hostnames, DNS servers, and IP addresses change rapidly – within minutes or less. Each of these rapid changes serves to immediately move the botnet advertised website or email source to a different location in an entirely different country.

These domains are used to track and control botnets, host malware payloads, repositories for other harmful content such as child pornography, host websites for phishing, pills and other spam content.

[78] http://www.honeynet.org/papers/ff/index.html

This technique also defeats the traditional method of botnet take down – going after individual command and control servers, and after individual hosts in a botnet, and trying to take them all down one at a time.

Domains used for botnets can have several DNS servers (all hosted on botnet hosts, for extra resiliency), and several IP addresses that they randomly cycle through in minutes. Quick take down of a single command and control center, or a single phish website, is rendered almost impossible, as the location rapidly changes from IP to IP, and country to country.

The “Rock” phish kit uses a related technique.  Rock is a readymade phisher's toolkit that can set up an entire phishing campaign out of the box, customized to a wide variety of banks and financial institutions.  The right set of templates can create an authentic copy of different banks for the same phisher – so the same spam infrastructure, the same botnets, the same website hosting can be quickly recycled to phish an entirely different bank or financial institution each time.

The Rock Phish kit uses a large number of proxies (all compromised botnet hosts, that get a proxy server installed onto them), in order to hide the location of a smaller number of critical servers. Anyone visiting a rock phish site would initially see his computer connected to a botnet computer – which then immediately redirects him to the actual site.

Botherders routinely use fast flux and Rock Phish style proxies to protect their own critical infrastructure – their command and control centres, their repositories for stolen data, phishing websites, payment gateways – anything that is critical to the survival of their botnet, or to their earning money from the botnet's activities.

## The Role of Registrars and Registries

Domains used for botnets, spam and malware are invariably fraudulently registered,  using stolen credit cards, and have a whois record that is either entirely fake (quite often, the identity of the credit card owner gets listed in the whois for such domains), or “cloaked” using anonymous domain registration facilities that several registrars provide.

It should be noted that anonymous domain registration is an entirely legitimate service introduced by registrars, and is meant to protect the privacy of legitimate domain owners, much on the lines of unlisted numbers in telephone directories. Of course, spammers and botherders gleefully exploit this extra layer of anonymity to further conceal their traces and delay detection.

Botherders and spammers routinely register several hundred domains per campaign at a single registrar, or under a single ccTLD. If the registrar or ccTLD does not have, or enforce, a policy to take down such domains, the infestation of such domains on their service increases as more botnet operators and spammers move their domains there.

In some cases, spammers and botherders may attempt to set up a bogus registrar, so that they can process registrations for their own domains themselves. Quite often, this is accomplished simply by becoming a reseller of a larger registrar with lax policies and insufficient control or oversight on the activities of their resellers, as this is an easier method for the botherder than seeking ICANN accreditation to become a registrar themselves. They are also known to establish fake ISPs[79] to provide hosting and network connectivity to a wide range of malicious activities.

While domains are apparently a more distributed method of command and control given the high degree of redundancy and robustness that characterizes DNS, they are themselves a single point of failure, as a quick take down of domains registered for a botnet campaign leads to a temporary collapse of the campaign. It also leads to the inability of the spammer or botherder to profit from his activities, as he loses control of his botnet, and once the domain is terminated, nobody can access the malware, child pornography or phishing site that was hosted on the domain.

This situation makes it imperative to extend the nodal agency facilitated watch, warning and incident response mechanism discussed earlier in this

[79] http://www.spamhaus.org/Rokso/listing.lasso?-op=cn&spammer=Russian%20Business%20Network

paper to extend to registries and registrars based in a country, in order to channel take down requests quickly and efficiently to the relevant registrar or registry.

An example of how well such a notification model can work is a recent joint effort by the .hk ccTLD registry Hong Kong Domain Name Registration Company Limited (HKDNR)[80], and Hong Kong's Office of the Telecommunications Authority (OFTA)[81] to take down several thousand domains under the .hk ccTLD. These domains were registered by botnet operators and used to operate botnet hosted websites that advertised fraudulent prescription drugs, phishing scams and bogus stock advisories for “pump and dump” scams.

OFTA obtained automated feeds of such domains from various private stakeholders involved in tracking spam and botnets, and worked with HKDNR to develop guiding principles for the take down of such domains. An indicator of their success, and of the scale of the problem that HKDNR tackled and is successfully mitigating, is that they were able to suspend over 2000 such domains in a single day.

Besides active participation in local Watch, Warning and Incident Response Systems, registrars and registries should be encouraged to communicate with each other and share information about incidences of spam and botnet domain registration on their systems. Existing loopholes that allowed such domains to be signed up can be plugged, and the results shared with their peers Registrars and Registries are also encouraged to take steps against domain registration using stolen identities and stolen credit cards, using industry best practices to mitigate fraudulent transactions, as well as reasonable know your customer norms.

[80] http://www.hkdnr.hk
[81] http://www.ofta.gov.hk

## Whois Privacy and Domain Takedowns

As has been mentioned earlier in this paper, especially in the case of botnets, domain names used by the botnet are quite often the single point of failure where a decentralized botnet can be taken down. Therefore, strong emphasis is placed on developing guidelines and standard operational procedures in order to quickly and efficiently taking down domains that are used for botnets, malware, child pornography, and other net abuse.

For both ISP / blocklist antispam investigators and for law enforcement officers investigating spam and botnet cases, one of the most potent tools for tracing ownership for a particular domain is the whois records showing registration information for the domain. Even in cases where the whois information is entirely fake, with completely bogus information in the whois record for a domain, a pattern may emerge in the forgeries used, that would make it easier for law enforcement to tie different domains owned by (say) a single botnet gang together.

Conversely, there is a widely held view that whois records must be entirely suppressed, or at least restricted to an “Operational Point of Contact” for the domain, as a privacy measure. This too has points in its favor – the right to anonymous free speech on the Internet and the risk of having whois records mined by spammers are among the two most commonly cited reasons to restrict whois data. However, the vast majority of domains are registered by commercial entities, for commercial purposes, rather than by individuals. Further, commercial speech is typically subject to greater limitations than, and enjoys far more limited protection, if at all, compared to individual freedoms of speech and expression.

Privacy laws including the right to anonymity invariably apply to individuals (natural persons), not to legal persons (business entities, non profits, organizations), and restricting access to whois for all domain names to protect the privacy rights of individuals (who register a tiny fraction of the domain names currently in circulation) can possibly be reconsidered.

There are alternative mechanisms available in several ccTLDs that allow the suppression of whois information for personal domains, with a mechanism similar to the register provided proxy/anonymous whois registration services currently in place.

It has become apparent that spammers and botherders will actively abuse well-intentioned measures aimed at protecting the privacy and free speech rights of the individual.  This abuse facilitates the active spread of spam and botnets by enabling them to evade detection, and this eventually leads to even grosser, criminal violations of people's privacy, acts such as identity theft and extortion.

Restricting whois privacy to individual domain name owners (natural persons, using their domains exclusively for non commercial purposes, as opposed to business entities) still leaves open the potential for malefactors to falsely declare that they are individuals, or to use the contact data of individuals whose identity and credit cards have been stolen by them in domain registrations.

An OECD paper[82] released in 2003  highlighted these and various other consumer policy considerations that are quite valid and applicable to formulate policy on the display of whois information about commercial domain names, consistent with the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce (1999).   As pointed out in this paper:

- Accurate whois records complement accurate contact information on a website as key elements that facilitate easy identification of the business entity that a consumer is dealing with online.   Further, consumer protection enforcement may require the enforcement authority to easily locate the physical presence of an online business.

[82] http://www.olis.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/98f97d6ef9579165c1256d39004ceb73/$FILE/JT00145317.PDF

- Businesses that deliberately provide bogus contact information in whois are quite unlikely to provide valid contact information on their website. The OECD guidelines therefore ask that businesses do not “exploit the special characteristics of electronic commerce to hide their true identity or location, or to avoid compliance with consumer protection standards and/or enforcement mechanisms.” [Part Two, II] and that “online businesses should provide: “accurate, clear and easily accessible information about themselves sufficient to allow, at a minimum ... location of the business and its principals by law enforcement and regulatory officials.” [Part Two, III(A)].

- OECD member countries are also committed to “the protection of privacy on global networks in order to ensure the respect of important rights, build confidence on global networks, and to prevent unnecessary restrictions on transborder flows of personal data” (OECD, 1980, 1998). The public disclosure of Whois contact information about domain names registered for **non-commercial** purposes raises important privacy issues. ... The consumer protection issues discussed in this paper concern **commercial** Web sites. For online businesses, disclosure of professional contact information (e.g. name, a work e-mail address or telephone number) should not pose a danger to privacy and individual liberties where the individual is acting as a representative of an online business.

There is ongoing discussion in the ICANN GNSO / Whois Task Force[83], and in other forums, on this issue. There is a clear division of opinion - privacy advocates and groups focused on data protection stress the right to anonymity on the Internet.

A contrary opinion and reservations as to the consequences of such anonymity being abuse is expressed, in varying degrees and citing various

[83] http://gnso.icann.org/issues/whois-privacy/
http://gnso.icann.org/issues/whois-privacy/whois-services-final-tf-report-12mar07.htm

reasons, by antispam advocacy groups, law enforcement organizations and coalitions of trademark / intellectual property rights advocates.

Significantly, the ICANN Whois Working Group's final report[84] agreed that the OPOC proposal should change WHOIS policy on publication of data to distinguish between natural persons, where there would be only limited public display of WHOIS records, and legal persons for which there would be full display.

During the ICANN GNSO meeting[85] at Los Angeles on 31 October 2007, the OPOC proposal was rejected by 7 yes and 17 no votes, while an alternate proposal to introduce a sunset period for whois, and eliminate whois requirements from contracts in a year if consensus was not reached – an attempt to force negotiation - failed by a narrower margin, 10 yes to 13 no votes.

During this meeting, the GNSO acknowledged that further research is required on the technical and cost wise feasibility of several proposed approaches, which, the whois working group and subsequently GNSO have determined, will require further study[86].

There is also the consideration of how to distinguish between a natural and a legal person at the time of registration, as well as how to determine whether a natural person will not use the domain to carry out commercial activities once the domain is registered.

Consensus needs to be developed on the viability of preserving anonymity in whois, but putting in place mechanisms to mitigate the abuse of such anonymity, and where needed, enable law enforcement to follow up on such abuse of whois anonymity for the purpose of cybercrime such as spam, malware and botnets.

[84] http://gnso.icann.org/drafts/icann-whois-wg-report-final-1-9.pdf
[85] http://gnso.icann.org/meetings/agenda-31oct07.shtml
[86] http://gnso.icann.org/drafts/icann-staff-overview-of-whois11oct07.pdf

Further, registrars and registries will need to develop best practices on the mitigation of fraudulent registration of domain names for abusive purposes and on the quick location and take down of such domains in order to mitigate the harmful activities that are facilitated by the abuse of such domains.

The following submissions may be of interest in this context:

- *Presentation by OPTA Netherlands on "The Importance of Whois Databases for Spam Enforcement"*: http://www.icann.org/presentations/opta-mar-26jun06.pdf
- *Memorandum from the Anti Phishing Working Group*: http://www.antiphishing.org/reports/APWG_MemoOnDomainWhoisTake-Downs.pdf
- *Comments from the Coalition Against Unsolicited Commercial Email (CAUCE)*: http://forum.icann.org/lists/whois-services-comments/msg00036.html
- *Final report of the ICANN whois working group*: http://gnso.icann.org/drafts/icann-whois-wg-report-final-1-9.pdf

## A Parallel Case – Open Relays in the Past

The debate on openness in domain name whois records is similar to a previous online debate on the availability and use of open relays on the Internet. Open relays were originally intended as a courtesy measure, in an age when mailservers typically had limited connectivity to each other, so that open relays were used by servers to reach other servers they were not directly connected to.

Open Relays were also actively encouraged as a way out for Internet users who were away from their homes but still wanted the ability to send out email. All this was perfectly true in the years before web based email services like Hotmail, and SMTP authentication to enable roaming users to continue to use their email provider's SMTP servers, became available or in wide use. Open Relays became widely unpopular after spammers began to abuse them (starting from the mid 1990s).

The parallel with whois and anonymity is even more pronounced when it is noted that spammers particularly valued “anonymous” open relays, running software that was either outdated, or misconfigured, and so would not log the sender's IP address. Mailservers that normally are not open to relaying might, in certain cases, become open, or even anonymous open relays if various automated configuration tools supplied by the operating system vendor or third parties were incorrectly used to configure them.

Open relays were quite common until around 2001, after which vendors began to secure the default mail server configurations in their operating systems, and in some cases, disable the mail server unless specifically enabled by the server's administrator.

## *Best Practices for e-Commerce, Online Banking, Auction and Payment Sites*

### High Risk, Attractive Targets for Fraud and Cybercrime

E-commerce websites, that transact the bulk of their business online, are favorite targets for botnets. These websites are mission critical for online businesses, so that even a few hours of downtime can lead to massive financial losses. Thousands of people around the world make transactions online using their credit cards. Regular users of a website may create accounts on the site, with a user profile that stores their personal data such as their name, address, credit card number. All these factors make e-commerce and financial websites attractive targets for cybercrime.

Botnet operators routinely issue extortion threats to the operators of such sites, threatening to use botnets and launch DDoS attacks against them unless a ransom is paid. As has been mentioned earlier in this paper, three Russian citizens were imprisoned for extorting millions of dollars from sports betting sites, threatening to disrupt their business by DDoS attacks if a ransom was not paid.

Password cracking and other intrusion attempts, again using the massively distributed computing power of a botnet, has led to several massive, well publicized security breaches at various sites, causing billing databases with several hundred thousand user profiles (names, addresses, email addresses, credit card numbers) being hijacked.

Besides such large scale identity theft, users of e-commerce sites are routinely targeted by botnets that deploy phishing spam campaigns, trying to steal passwords and personally identifiable information from them. Botnets are further used to deploy keyloggers and other malware (such as screen scrapers, which capture every single change visible on the screen when the user visits an e-commerce or online banking site).

Transactions involving the purchase of expensive goods (luxury goods, first class air tickets, and holidays at resorts) are routinely made on e-Commerce sites using stolen credit cards, enabling scam artists to profit from credit card theft, as well as to hide their own identity when making the transaction. One variant of this scam offers expensive goods such as laptops for sale on auction and classified ads websites, with the offer price lower than market rate (a USD 2500 laptop might be offered for USD 2200). A stolen credit card is used to buy a laptop, and this is then shipped to the winning bidder. The scammer receives his USD 2200 through a stolen online money transfer account.

Stolen accounts on online money transfer services such as Paypal are widely used to make rapid electronic transfers of stolen money, moving it offshore in the first step of the money laundering process. Similarly, stolen accounts on online share trading services can be used to make bogus transactions on penny stocks, as part of a “pump and dump” stock scam.

### Security Best Practices for e-Commerce Sites

Banks and e-commerce sites are encouraged to follow widely accepted best practices including secure network design, updated systems security measures, strict password / two factor authentication and physical security of the system and network, especially parts of the network where customer data is stored, isolation and encryption of customer databases, deployment of strong cryptography in order to encrypt website traffic etc.  These measures should be backed by a stringent set of auditing procedures.

E-commerce and financial sites make attractive targets for DDoS, and are strongly encouraged to deploy mitigation measures, such as multiple redundant links to the Internet, ideally from “security aware” providers who can filter and mitigate DDoS traffic to some extent “upstream” of the site – before such traffic reaches the site.  In addition, they should deploy dedicated DDoS mitigation equipment and policies as part of their network and disaster recovery plans.

Financial institutions and e-commerce vendors that operate online are urged to form local CSIRT / CERT teams that work with the institution’s IT security team in order to carry out security audits, as well as engage in watch, warning and response systems in order to facilitate quick detection and blocking and/or take down of DDoS sources.

### Customer Education and Safety

Educational campaigns are deemed necessary to sensitize their customers to phishing and other scams, and to inform them of the need for good password security.

Increased client security, such as strong passwords, or the deployment of two factor authentication using hardware tokens to generate a random one time PIN number that has to be entered along with the usual login and password, which is popular in the banking industry, are highly recommended as well.

Another such technique (deployed, for example, by Yahoo) is to allow the user to specify an icon (such as a picture of himself, or one of a selected set of icons that the portal allows him to choose from) – the user is then assured that when he sees a login screen in which his icon is displayed, he is actually visiting the actual portal and not a phishing site.

Furthermore, increased loss prevention measures to mitigate losses due to credit card fraud, in cooperation with banks, card issuers and credit report agencies, as well as internal processes such as implementing know your customer norms and validating credit cards associated with user profiles, are strongly suggested.

Additionally, e-commerce vendors are encouraged to deploy additional validation mechanisms such as “Verified by Visa” and “Mastercard Securecode”, in which the transaction is carried out only after the customer validates it with a pre-agreed password that he has set up with his credit card provider.

An example of the effect that card fraud and the resulting loss of confidence in the online payment process can have in stifling online commerce is that several airline and air ticketing websites in India recently stopped accepting foreign credit cards, due to stolen international cards used to book air tickets, which were then resold cheaply to the general public by some corrupt travel agents.

Providers are strongly encouraged to widely deploy captcha and other techniques to deter automated or scripted signup by spammers and other malefactors, as well as have manual and automated checks in place to enable quick detection and take down of bogus accounts created by fraudsters, and deactivation of stolen accounts in order to mitigate their abuse. Users whose accounts are stolen can then be notified. Automated processes that can be used to watch out for bogus accounts include checks for multiple accounts signed up from the same IP address, or with the same pattern of usernames/ passwords.

E-Commerce providers are encouraged to deploy and use email authentication mechanisms such as DKIM (Domain Keys Identified Mail) and the Sender ID Framework, as well as other reputation assurance mechanisms, such as out of band whitelisting with Internet providers, in order to provide a way for their valid email to be distinguished from fraudulent phishing spam that forges the portal's name and style to dupe users into giving up their password and other personal data.

ISPs and e-commerce vendors need to cooperate in order to ensure that legitimate and solicited emails from the e-commerce provider are not treated as spam by the ISP. For example, eBay and Paypal have announced[87] that they will sign all their email with DKIM, and any email that claims to be from them but is not so signed can be safely treated as spam.

Similarly, e-Commerce providers must ensure that their email marketing campaigns respect the privacy of ISP users, so that these campaigns do not trigger spam complaints from the users which may then trigger a block. MAAWG members from both their ISP and email marketing / e-Commerce provider membership constituencies have jointly put together a "Sender Best Current Practices"[88] document that suggests ways and means by which this can be accomplished.

At a national level, ISP to Industry/e-Commerce portal interaction can be facilitated by local and regional chambers of commerce, IT industry advocacy groups and similar bodies. Local ISPs and e-Commerce/email marketing vendors are also encouraged to consider joining international initiatives such as MAAWG and APWG, besides actively pursuing regional cooperation initiatives.

Some banks declare to their users that all online communication with the bank will not be sent through email, but through a contact form built into the bank's secure online banking website, and replies from the bank will be displayed on the same website, not sent back in email. Further, banks restrict several key transactions from being completely carried out online – a form may have to be faxed into the bank, or the user may have to go personally to a branch.

[87] http://www.networkworld.com/news/2007/032707-paypal-asking-e-mail-services-to.html

[88] http://www.maawg.org/about/MAAWG_Sender_BCP/

In some cases, banks may employ an out of band verification step.  When a request is placed, the bank mails out a code to the customer's postal address or text messages it to his registered cellphone.  That code has to be entered into the bank's website in order to complete the transaction.

It must be pointed out that none of the strategies discussed above are completely foolproof, or guaranteed to totally eliminate the problems that botnets can create for security.  They are all methods to mitigate the risk that businesses and consumers are exposed to when doing business online. Further, an equitable balance will have to be struck between security and usability – it is quite possible to secure a system so well that while it may well be difficult for a botnet to penetrate it, it also becomes extremely difficult for the general public to access and use it.

# Annex C – Social

Initiatives in this area are already being pursued under WSIS Action Lines C2 (Information and Communications Infrastructure), C4 (Capacity Building) and C6 (Enabling Environment). A short section of suggested measures relevant to the context of botnets, and generally of WSIS Action Line C5 (Building Confidence and Security in the use of ICTs) is provided below. Much more detailed material is available as part of other projects and documents prepared under these WSIS action lines

## *User Education and Awareness Raising Campaigns*

The effects of botnets and their consequences (spam, phishing, malware) are felt much more strongly by a public that lacks awareness on Internet safety. There is a need for sustained, widespread awareness raising and education campaigns that make strong use of visual media such as cartoons, posters and educational short films shown on television and in movie theaters. These will also need to be made available in the local languages spoken in various regions, besides the ITU official languages. Previous examples of this approach have included an initiative by the Dutch government to teach password security and other Internet safety measures through a Donald Duck cartoon.

Awareness raising campaigns through visual media have to be complemented with newspaper articles that cover such issues from a local angle, for example, interviews with victims of online fraud and identity theft campaigns accompanying informative articles on safe online behavior. Further, newspapers and PC magazines can be used to distribute CDs that have freely available security, antivirus and other software to their readership.

This has to be backed by introducing information security and safe online behavior as a part of the curriculum, starting from basic computer courses in schools to integration of information security, cybercrime and other related topics into graduate and post graduate degree courses. An example of this is an Information Security Education and Awareness project[89] launched by the Government of India's Ministry of Communications and Information Technology.

Developing economies typically have lower rates of PC and Internet penetration at home, so that a majority of users in such economies access the Internet at work or school, as well as from public access locations such as Internet cafés and libraries. Such public access locations where hundreds of people may access the Internet are at substantial risk of infection due to unsafe use of these resources and installation of pirated software in order to cut costs. Public access Internet locations should be reached out to (for example through Internet café industry groups, chambers of commerce and state education authorities) as distribution points for educational literature and short films prepared as part of an awareness campaign against botnets.

Civil society groups such as PC user groups and the Internet Society (ISOC), that already have education programs in place, should be reached out to, to enable integration of online security concepts in their programs where necessary. This will extend the benefits of existing programs in this field to a broader audience within the country and provide support in translating program material into the local language, venues where courses based on such material can be taught.

ISOC has an extensive archive[90] of material from workshops organized around the world on network operations, security and ICT. They provide an international event calendar for workshops, tools to plan educational programs, a database of instructors and peer review of training curricula.

[89] http://www.mit.gov.in/default.aspx?id=808
[90] http://ws.edu.isoc.org/

## *Provision of Access to Secure ICT Resources*

Locations that totally lack ICT of any sort are a tabula rasa, a clean slate from which to start projects which ensure that ICT access provided to the general public is secure.  The need for security provisions in products that provide ICT to a target audience that is completely unexposed to ICT before, either due to childhood and being beginners in the use of a computer, or due to a previous lack of access to ICTs and the Internet, induced by poverty, geographic location or other barriers to access.

Groups such as the One Laptop Per Child (OLPC)[91] project, that concentrate on providing ICT access to the masses will have to be reached out to, to ensure that they incorporate best practice measures to ensure secure computing use and Internet access in the devices that they distribute.

The need for adequate filtering is demonstrated by the fact that laptops provided by OLPC to schools in Nigeria were found to be used for surfing pornographic sites[92].  While there are a large number of legitimate websites focused on pornography, botherders routinely send out spam advertising explicit pornography (quite often of the illegal variety, involving rape and child exploitation), and further, use ad banners, browser exploits and other methods to download malware onto the computers of visitors to such sites.

Another example is the rapid rollout of Internet access to middle and high schools in several countries over the last few years.  There have been several cases where insecure and outdated software was deployed by schools given such Internet access, or in the case of Korean schools around 2000-02, a standard Internet access gateway was deployed across a large number of schools, and this gateway apparently included an open proxy server that allowed the proxying of spam. Spammers quickly grasped the opportunity that this misconfiguration offered and began to actively seek out and abuse

[91] http://laptop.org
[92] http://africa.reuters.com/wire/news/usnL19821905.html

school Internet connections around the world, until they were secured by the deployment of updated software.

These are experiences that need not be repeated.  Organizations developing public access computing resources and Internet gateways that will be deployed in schools and other shared access environments (such as Internet cafés, hotel and airport business centers, public libraries, as well as Wifi hotspots or campus and city wide Wifi networks) should be actively reached out to, in order to ensure that security features are integrated throughout the life cycle of a public access ICT project.

## *Cheaper and Open Source Alternatives to Pirated Software*

It is widely recognized that pirated software is especially susceptible to malware, as it comes from tainted sources so that even newly installed software might be infected.  Moreover, such software cannot be updated with security and other patches – a step taken by software vendors to discourage piracy, but one which not many users of pirated software particularly care about as they may not be aware of the need to upgrade software.

There are several cheaper or free alternatives to proprietary software including operating systems, office and email applications, antivirus etc and these present viable alternatives to current users of pirated software.  Such applications can be categorized as Shareware (which is free for a period of 30 days, after which it must be purchased and registered), Freeware (which remains free, possibly with reduced features compared to a paid version) and Free/Libre and Open Source Software.

However, most people remain unaware of these products, due to their being comparatively unknown and unadvertised brands, or because they may be perceived as less easy to use than products that are dominant in the market. Such software alternatives can be popularized by ICT organizations providing access to users, as well as by ISPs who provide free software to their users as CDs or downloads on their website.

### Free/Libre and Open Source Software

Free/Libre and Open Source (FLOSS) software, including Linux and most Linux based software, may present a cost effective alternative to proprietary software, in desktops as well as on servers and firewalls. FLOSS software is freely available for download and distribution, with the source code used to build these in the public domain so that it is open to free use as well as customization, under the terms of various licenses[93] such as the GNU GPL, Apache Software License, BSD License, Apple Public Source License etc.

The use of FLOSS software is certainly a much more acceptable alternative to provide access to ICT resources for people and countries that lack adequate financial resources, than the much more widely used, but insecure and illegal alternative – pirated versions of proprietary operating systems.

The effective license cost of FLOSS operating systems and software is zero – whereas legal versions of most proprietary server and desktop operating systems, firewalls, antivirus and antispam software is far higher, especially when the original price (in US dollars) is translated to the equivalent in local currency. This high cost of proprietary software further fuels a demand for pirated software, admittedly much more vulnerable to viruses and botnet activity as such software normally does not have access to updates and security patches, and moreover, may come preinstalled with a virus or trojan.

Several large ISPs and email providers around the world use FLOSS software and operating systems on their servers (for example Yahoo uses a customized version of the qmail mail server on FreeBSD and AOL uses a heavily customized version of sendmail). FLOSS software firewalls (such as IPtables) and proxy servers (such as Squid) are widely used to provide

[93] http://freshmeat.net/faq/view/48/

secure Internet access for several homes and small businesses, as well as at several ISPs and email providers.

FLOSS software also provides a usable desktop, with browsers, email, instant messaging, office productivity and other essential software readily available in a default install of Linux.  These tend to be regarded as reasonably secure, for various reasons including that they are not vulnerable to a large number of viruses that predominantly target other operating systems and turn infected PCs into the members of a botnet.

The cost equation and other reasons have certainly influenced some governments to encourage FLOSS software, and to deploy and use FLOSS within their own organizations.  A recent example is provided by the Electronics Corporation of Tamil Nadu (ELCOT), an organization owned by the government of Tamil Nadu state in India, which has deployed FLOSS technologies on a large scale, equipping state government office PCs with Linux and providing laptops preinstalled with Linux to officers of the Indian Administrative Service[94].  ELCOT has further designed cheap and secure ATM cash machines based on Linux[95], for deployment in small rural banks.

[94] http://mandriva.blogspot.com/2007/01/tamil-nadu-india-may-shut-door-on.html
[95] http://www.thehindu.com/2007/04/04/stories/2007040404760300.htm