CSRIC

Communications Security, Reliability and Interoperability Council

December 2010

FINAL REPORT

Internet Service Provider (ISP) Network Protection Practices

Working Group 8

Table of Contents

1 Executive Summary

Working Group 8 of the Communications Security, Reliability, and Interoperability Council (CSRIC) addressed the area of Internet Service Provider (ISP) Network Protection, with a focus on addressing "bots" and "botnets", which are serious and growing problems for end-users and ISP networks. Botnets are formed by maliciously infecting end-user computers and other devices with bot (from the word "robot") software through a variety of means, and surreptitiously controlling the devices remotely to transmit onto the Internet spam and other attacks (targeting both end-users and the network itself).

The Working Group examined potentially relevant existing Best Practices (BPs), and in consultation with industry and other experts in the field, identified additional Best Practices to address this growing problem.

The Working Group identified 24 Best Practices to address protection for end-users as well as the network. The Best Practices, set out in Appendix A, are organized into the logical steps required to address botnets. The first step is Prevention (12 BPs), followed by Detection (5 BPs), Notification (2 BPs), and then Mitigation (3 BPs). In addition, 2 BPs on Privacy Considerations were identified to address the handling of customer information in botnet response. The BPs identified are primarily for use by ISPs that provide service to consumer end-users on residential broadband networks but may apply to other end-users and networks as well.

Industry participants are encouraged to have their respective subject matter experts review these Best Practices for applicability. It is critical to note that Best Practices in general are not applicable in every situation because of multiple factors, and such a caveat applies to the work product of the Working Group. Therefore, the Best Practices set out below are intended to be voluntary in nature for ISPs, and may not apply in all contexts (and thus for a host of reasons should not be made mandatory). With this understanding, the Working Group recommends that the Best Practices be implemented by ISPs, where applicable, in order to address the growing botnet problem in consumer end-user devices and ISP networks.

2 Introduction

The Communications Security, Reliability and Interoperability Council ("CSRIC) is a Federal Advisory Committee that provides input and recommendations to the Federal Communications Commission ("FCC") regarding the security, reliability and resiliency of communications systems, including telecommunications, media and public safety communications systems. On March 19, 2009, the FCC, pursuant to the Federal Advisory Committee Act, renewed the charter for the CSRIC for a period of two years, through March 18, 2011. The FCC commenced its first set of CSRIC meetings in December, 2009.

CSRIC created ten working groups, each with its own area of responsibility. As a result, Working Group 8 was charged with producing a report regarding ISP Network Protection Practices with a focus on botnets, a significant and growing problem in ISP cybersecurity.

Working Group 8 began bi-weekly discussions on March 8, 2010. The group members represent a wide range of expertise in network protection and consumer use of computers. (See

Section 2.2.) In addition to the bi-weekly calls, the group met face to face twice in Washington, DC. The Working Group's scope of effort is described in Section 3.

After efforts to scope the problem, the Working Group turned to other industry experts to evaluate the current situation with respect to network protection and infected computers. The Working Group heard from representatives of Neustar, the Spamhaus Project, Damballa, Messaging Anti-Abuse Working Group (MAAWG) and the National Cyber Security Alliance. The information garnered from these experts formed the basis for many of the Best Practices identified by the Working Group.

The Working Group further refined its scope in order to address the botnet problem effectively. As the Working Group identified areas to address, it recognized that the most pressing area of the botnet problem lies in consumer-focused residential broadband networks. Although botnets are also a concern with business-focused networks and service, the business arrangements in that context are far more diverse than in the residential consumer market, and there is already more activity in the business context in response to botnets. Our focus for this Report is thus on identifying Best Practices for ISPs that provide services to consumers on residential broadband networks.

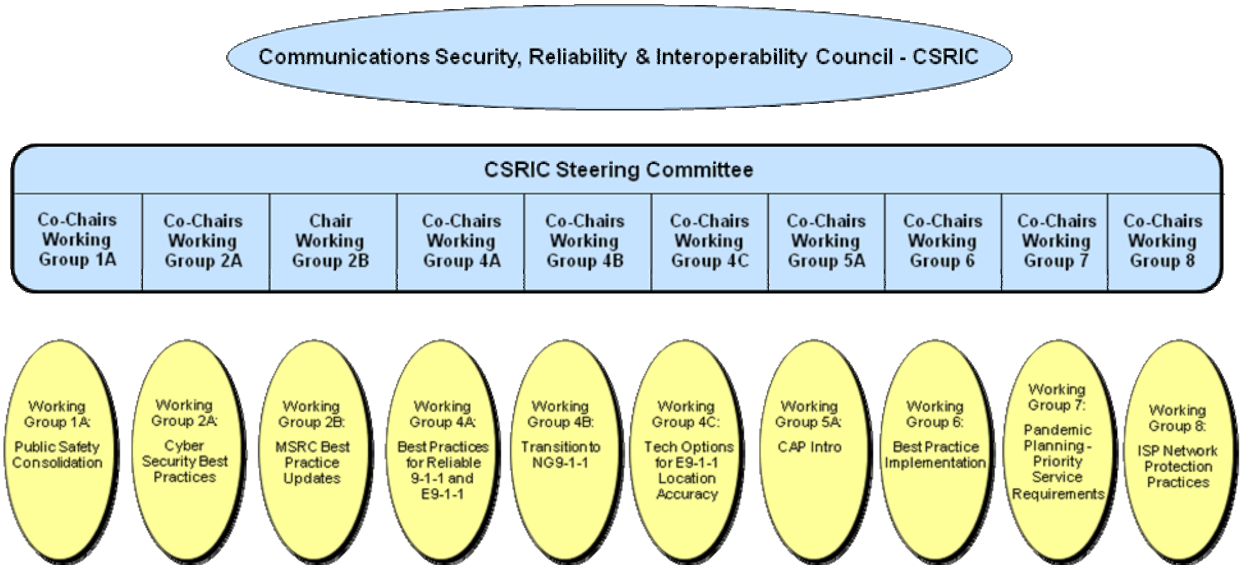
Notwithstanding this focus, many of the Best Practices identified here would also be valuable practices to apply in non-consumer, non-residential network contexts. The Working Group recommends that, at a later date, the FCC consider whether additional best practice work would be valuable in these areas.

The Best Practices suggested in this Report reflect the consensus of Working Group 8 as to measures that ISPs should *voluntarily* undertake to address the botnet problem on residential broadband networks. The Working Group specifically did not undertake to make any recommendations of any measures for which it should be *mandated* that service providers implement. In light of the complexity and diversity of individual networks, and the fast-changing nature of the botnet security threats, individual networks should be able to respond to security threats in the manner most appropriate for their own network.

The Best Practices should not be viewed as an exhaustive list of all steps that ISPs could take to address botnets and compromised computers. Indeed, many service providers take additional steps in response to the botnet problem, and many are often assessing what new or additional techniques should be considered – beyond the foundational measures suggested below.

As noted, the Best Practices identified below reflect the consensus of Working Group 8, arrived at through a collaborative process of discussion and refinement. The background and overview of the botnet problem and the Working Group's process and discussions were prepared primarily by the Working Group co-chairs in consultation with the Working Group members, but may not reflect in all details the consensus of all members of the group.

2.1 CSRIC Structure


Communications Security, Reliability & Interoperability Council - CSRIC
CSRIC Steering Committee
Co-Chairs Working Group 1A
Co-Chairs Working Group 2A
Chair Working Group 2B
Co-Chairs Working Group 4A
Co-Chairs Working Group 4B
Co-Chairs Working Group 4C
Co-Chairs Working Group 5A
Co-Chairs Working Group 6
Co-Chairs Working Group 7
Co-Chairs Working Group 8
Working Group 1A: Public Safety Consolidation
Working Group 2A: Cyber Security Best Practices
Working Group 2B: MSRC Best Practice Updates
Working Group 4A: Best Practices for Reliable 9-1-1 and E9-1-1
Working Group 4B: Transition to NG9-1-1
Working Group 4C: Tech Options for E9-1-1 Location Accuracy
Working Group 5A: CAP Intro
Working Group 6: Best Practice Implementation
Working Group 7: Pandemic Planning - Priority Service Requirements
Working Group 8: ISP Network Protection Practices

2.2 Working Group 8 Team Members

Working Group 8 consists of the members listed below:

Name	Company
John Morris (Co-Chair)	Center for Democracy & Technology
Richard Lynch (Co-chair)	Verizon
William Salusky	AOL
Mike Recchia	AT&T
Tim Battles	AT&T
Robert Thornberry	Bell Labs, Alcatel-Lucent
Neil Schwartzman	Coalition Against Unsolicited Commercial Email (CAUCE)
Jason Livingood	Comcast
Doug Davis	Comptel / HyperCube Telecom
Brian Moir	E-Commerce, Telecommunications Users Group(e-TUG)
Pete Fonash	Federal Reserve
Richard Hovey	FCC
Eric Davis	Google
Jeff Williams	Microsoft
Kevin McGuire	NTCA
Paul Diamond	Qwest
Michael Fiumano	Sprint – Nextel
Damon Dowdall	Sprint – Nextel
Vince Weafer	Symantec

Nick Lordi	Telcordia Technologies
Barry Harp	U.S. Department of Health and Human Services
Delano Marshall	U.S. Department of Health and Human Services
David Young	Verizon
Marcus Sachs	Verizon

Table 1 - Working Group 8 Members[1]

3 Objective, Scope, and Methodology

3.1 *Objective*

This document addresses the objective and deliverables outlined in the charter for Working Group 8, as defined by the full CSRIC:

> Working Group 8 has investigated current practices that ISPs use to protect their networks from harms caused by the *logical* connection of computer equipment, as well as desired practices and associated implementation obstacles[2]. These efforts address techniques for dynamically identifying computer equipment that is engaging in a malicious cyber attack, notifying the user, and remediating the problem. The Working Group has developed recommendations for CSRIC's consideration for best practices and actions the FCC could take that may help overcome implementation obstacles.

The Working Group focused its efforts on the relationship between ISPs and end users in the residential broadband context. The Working Group worked to understand the problem of botnet–compromised, end-user devices and identify Best Practices for ISPs that are effective in addressing end-user device compromise.

3.2 *Scope*

This section details the problem statement, working group description and deliverables outlined in the CSRIC charter for Working Group 8:

Problem Statement: Security flaws in the hardware and/or software used by consumers coupled with poor or non-existent system administration practices by end-users have resulted in an epidemic of compromised computers, many of which can be remotely controlled as a part of what are frequently called 'botnets'. Once compromised, the owners of these computers are put at risk as their personal information and communications can be monitored,

[1] Robert Thornberry of Bell Labs, Alcatel-Lucent, and Paul Diamond of Qwest served as the lead editors of the Best Practices themselves, and the Working Group Co-chairs appreciate the significant time, effort, and patience that this entailed. The Working Group Co-chairs would also like to thank Katherine O'Hara of Verizon for her invaluable efforts in helping this Group operate efficiently, and in the preparation of this Report.

[2] As used here "computer equipment" includes a wide variety of personal equipment (*e.g.*, servers, PCs, smart phones, home routers, *etc.*) as well as household devices with embedded IP network connectivity. "logical connection" refers to end-user data communications protocol signaling and transmission. Harms result from the ability to degrade the communications infrastructure though malicious protocol exchanges and information transmission.

and their computing power and Internet access can be exploited by those controlling the botnet. Armies of these compromised computers can also be used together to disseminate spam, store and transfer illegal content, and to attack the servers of government and private entities with massive, distributed denial of service (DDoS) attacks.

Working Group Description: This Working Group will investigate current practices that ISPs use to protect their networks from harms caused by the logical connection of computer equipment as well as desired practices and associated implementation obstacles. The work should address techniques for dynamically identifying computer equipment that is engaging in a malicious cyber attack, notifying the user, and remediating the problem. The working Group will develop proposed recommendations for CSRIC's consideration for best practices and actions the FCC could take that may help overcome implementation obstacles.

Deliverables:

1. Capture Best Practices that address ISP end-user device botnet compromise and mitigate the potential network impact on ISPs.
2. Investigate and assess the impact on privacy concerns related to botnet compromises and recommend best practices addressing these issues.
3. Develop a reference list that provides additional information related to these issues.
4. Recommend further work to address the botnet issues.

3.3 Methodology

3.3.1 *Methodology Overview*[3]

Working Group 8 began its investigation by conducting research into the state of botnets, the extent of compromised devices and the effects on end-users and the network. The Working Group evaluated existing Best Practices for relevance and incorporated those that were determined to be effective and implementable. New Best Practices were created as needed, based on the information provided to the Working Group from industry experts (including members of the Working Group itself).

The Best Practices identified by the Working Group target ISPs that provide services to consumers on residential broadband networks. Many of the Best Practices suggested here, however, would also be valuable practices to follow in non-consumer, non-residential contexts. The Working Group recommends that, at a later date, the FCC consider whether additional best practice work is would be valuable in these areas.

3.3.1.1 Research

The Working Group research included consultation with industry experts. The Working Group invited representatives from Neustar, the Spamhaus Project, Damballa, Messaging Anti-Abuse Working Group and the National Cyber Security Alliance to present their findings, recommendations and insights into botnet prevention, detection, notification and mitigation.

[3] The Working Group heard from Mr. Karl F. Rauscher, NRIC Steering Committee Member and Best Practice Contributor, on using NRIC Best Practices as a model for developing CSRIC WG 8 Best Practices.

In addition to hearing from industry experts, the Working Group tapped expertise from within. For example, representatives from Coalition Against Unsolicited Commercial Email (CAUCE) provided insight into Best Practices. The Working Group also reviewed on-going research and documents developed within the Internet Engineering Task Force (IETF) to expand the group's understanding of the scope and breadth of botnets affecting end-users.

Based on the research conducted by Working Group 8, the following is a summary of findings from expert presentations and consultations:

- Botnet compromise of end-user devices is a significant problem that affects all ISPs - large and small.
- Botnet malware is rapidly proliferating into end-user devices.
- A rapid increase in botnet infections and technological sophistication appears to have been driven by the funding of botnet technology by sophisticated criminal elements.
- Botnet malware technology, infections, and the resulting impacts resulting from them are moving faster than ISP industry methods and technologies have, to date, been able to respond.
- Botnets are a complex issue involving both end-user and network issues.
- ISP efforts to address botnets must include cooperation and information sharing among ISPs in order to fully address the problem.
- There are existing Best Practices (including some IETF RFCs) that address certain aspects of botnets (e.g., concerning responses to spam), but no comprehensive approach has been identified or widely implemented in United States networks.
- Botnet detection methods raise issues of end-user privacy which need to be considered when developing approaches to the botnet problem.
- The problem of botnets in end-user devices can be substantially improved by implementation of the Best Practices identified by the Working Group, as applicable, by ISPs serving consumers on residential broadband networks.

3.3.1.2 Next Steps

The initial work of Working Group 8 sets a foundation for ISPs to address bots in end-user devices on residential broadband networks, helping to reduce the impact of botnet attacks on the network. Because of the immense scope of the issue, we have just scratched the surface. Possible next steps in dealing with bots and botnets could be to widen the scope of this work to include attack vectors which exploit network vulnerabilities to propagate bots and provide for obfuscation of botnet Command and Control channels. Although we touched on this area with our initial work in DNS, dynamic space, and spam, this work could be expanded to include improved protection from social engineering vulnerabilities, the infection of public web sites with bot-related Trojans and other malware, and further work on the network detection and isolation of bot Command and Control traffic. Work in some of these areas may fall outside te scope of CSRIC or the reach of the FCC, but could be pursued in other voluntary industry and multi-stakeholder fora.

As mentioned in the Recommendations section, these Best Practices should be reviewed frequently and updated to reflect the latest technology and methods in dealing with botnets. In addition, the Working Group recommends that, at a later date, the FCC consider whether additional best practice work would be valuable in network-focused areas beyond the residential broadband networks that formed the focus of this Report.

3.3.1.3 Creation of New Best Practices

In the work to create new ISP Best practices, we reviewed current NRIC Best Practices to identify any existing Best Practices that applied to our charter and to determine if these Best Practices needed modification or updating. Although we found two that referred to bots, they were focused on network issues that were out of our scope for this Working Group.

As new Best Practices were identified and created, the Working Group categorized the Best Practices in terms of the logical steps required to address botnets. The Best Practice categories identified by the Working Group include Prevention, Detection, and Notification of end-users, Mitigation, and Privacy Considerations in detecting bots and notifying end-users. The Best Practices are set out in Appendix A.

3.3.1.3.1 Prevention Best Practices

The twelve Prevention Best Practices are aimed at preventing botnet infections in end-user devices and major impacts to ISP networks. For end-users, the main focus is on how ISPs can help residential broadband end-users prevent bot malware infections from occurring in their devices and networks. This is accomplished by identifying Best Practices for end-user awareness and education of the importance of good Internet hygiene, e.g., keeping operating systems and applications up to date, being aware of social engineering scams, etc., and the use of anti-virus software to aid in malware and bot detection.   ISP personnel need to keep abreast of the latest botnet technology and malware in order to effectively address botnet issues. Network prevention Best Practices address bot exploits of the Domain Name System, dynamic address space, and the prevention of bot-originated spam (which helps to spread bots and other malware and create network congestion.)

3.3.1.3.2 Detection Best Practices

The five Detection Best Practices are aimed at providing effective ISP bot detection capabilities and sharing information among ISPs. Because of the increasing sophistication of botnets and the rapidly changing technologies being utilized in botnets, maintaining effective detection methods and sharing of information are critical to addressing botnet deployments. Also, the need for utilizing non-interfering detection methods and timely execution are also addressed.

3.3.1.3.3 Notification Best Practices

Once a bot infection is detected, the end-user needs to be notified so that mitigation action can be taken. The two Notification Best Practices are aimed at maintaining effective notification methods and ensuring that critical service information is conveyed to end-users who likely have a bot infection on their device or network. We suggest that a good balance be struck between the certainty of the detection and the speed of notification.

3.3.1.3.4 Mitigation Best Practices

Three Mitigation Best Practices are aimed at mitigating bots on end-user devices and the protection of end-users and the network from botnet attacks. Mitigation Best Practices address the need for the ISP to notify end-users by providing information on how to address a likely bot infection.   Best Practices are also identified for ISP cooperation in the face of critical cyber incidents that can be caused by a botnet attack, as well as the potential need for the temporary isolation of actively attacking bots to reduce the possibility of adverse end-user or network impact (recognizing that such action should only be used as a “last resort” or in other critical circumstances, and that any use should be sensitive to the needs of the affected users).

3.3.1.3.5 Privacy Considerations Best Practices

Some of the Prevention, Detection, Notification, and Mitigation Best Practices raise the recurring issue of protecting end-user information. To address these concerns, the Working Group developed two Best Practices focused on end-user privacy issues. The first deals with respecting consumers’ privacy with regard to exposed customer information in addressing bot infections and attacks and the second suggests a multi-pronged strategy in designing technical measures that protect the privacy of customer information.

4 Analysis, Findings and Recommendations

4.1 Analysis

The Working Group defined Best Practices in terms of the logical steps required to address botnets. Prevention Best Practices are those aimed at preventing botnet infections and the impact on ISP networks. Detection Best Practices are aimed at ISP detection of botnet infections and attacks. Notification Best Practices are targeted at notifying end-users of possible botnet infections. Mitigation Best Practices are aimed at mitigating end-user device botnet infections and the network impact.

4.2 Findings

Our investigation into botnet infections and attacks revealed a real and growing threat to both ISP end-users and ISP networks. We determined that botnets represent a rapidly shifting malware landscape of infection, command and control, and attack capability fueled primarily by the desire for economic gains by those who develop and deploy these botnets – often sophisticated criminals. We found that weaknesses in end-user devices as well as a lack of understanding and thus protective reactions by end-users themselves were largely responsible for the massive infections caused by sophisticated malware infection vectors.

Once infected with malware, botnets are formed when bot malware is activated on the infected device. The bot then establishes a connection with the botnet “command and control” system and then typically goes dormant to reduce the risk of detection while it awaits attack orders from the botnet owner. The level of sophistication has grown to the point where bots can often be updated with new versions of bot malware to add new attack capabilities and obfuscation techniques.

The botnet is comprised of all the infected bots under a common command and control. The bot malware itself is sometimes polymorphic, defying signature base detection at the device level. Use of sophisticated command and control mechanisms, including the use of peer-to-peer technology, make bot and botnet detection challenging. Command and control mechanisms exploit weaknesses in the ISP and Internet infrastructure, *e.g.,* DNS, to avoid detection of command and control traffic and to creatively provide infection vectors to spread the bot malware.

Once the end-user device becomes part of a botnet, threats exist to both the end-user and the ISP network. End-user personal information, such as identity, bank accounts, and credit card information, can be compromised; the ISP network can be exposed to denial of service attacks, spam, and other network related attacks.

To address these problems, the botnet lifecycle needs to be disrupted and mitigation of device bot malware needs to be addressed. The initial focus of this group was to look at end-user and end-user device issues, and some key network weaknesses that support botnet proliferation and exacerbate the impact of botnets.

Our findings suggest that the problem of botnets can be substantially mitigated by implementation, as applicable, of the suggested Best Practices in the residential broadband context. By looking at botnets from the perspective of Prevention, Detection, Notification, and Mitigation, a comprehensive program can be established which should have a significant impact on botnets and their impact on end-users and ISP networks. Most botnet control strategies we examined have some, but not all, elements of the Best Practices.

These findings support the original belief of the Working Group that botnet technology and deployment have, to date, moved faster than ISP industry methods to address them. One common theme within the findings is that cooperation with the end-user and other ISPs is critical in effectively dealing with this issue. There are no silver bullets that can completely eradicate this problem. Rather a partnership with end-users and other ISPs is required to address botnets in a comprehensive way.

4.3 Recommendations

The Working Group findings suggest that the rapid growth of botnets in end-user devices has been faster than the ability to effectively address the problem, hence significant work beyond the implementation of Best Practices is strongly encouraged. The following recommendations resulted from the research and Best Practice work of the Group:

- Because of the rapid growth of botnets and the rapidly changing technology, botnet Best Practices for ISPs should be revisited at least every two years.
- Standard methods for sharing information with end users and among ISPs should be better defined. This work could be led by the Alliance for Telecommunications Industry Solutions (ATIS) (http://www.atis.org/) and the U.S. Commerce Department's National Institute of Standards and Technology (NIST) (http://www.nist.gov/index.html)
- Protection (and discarding) of customer information that may be collected by ISPs while addressing botnets is an important issue that warrants continued attention.
- ISP implementation of the botnet Best Practices should be benchmarked to get a better idea how ISPs are dealing with the botnet problem.
- Additional possible policy actions are:
    - The creation, perhaps with government funding, of an anti-botnet website available to end users to assist in the removal of botnet malware from their device, similar to the anti-botnet centers created in Germany (see http://botfrei.de) and Japan (see, https://www.ccc.go.jp/en_ccc/);
    - The creation of a CyberSecurity public information campaign that includes botnet awareness;
    - The creation of a Computer Emergency Readiness Team (CERT) Information and Resource Center, available to ISPs and end users, devoted to botnet detection, mitigation, etc.; and

- Improvements in technology for network detection of botnet command and control and exploitation of traffic could be encouraged through research at NIST and research grants from Department of Homeland Security.

5 Conclusions

Working Group 8 identified 24 Best Practices to address bot-infected, end-user devices and the impact of botnets on end-users and ISP networks. These BPs form a foundation for addressing this growing problem and are for consideration by ISPs that provide service to consumers on residential broadband networks. Potential future work identified by the Working Group includes regularly reviewing these BPs to keep them up-to-date and to potentially expand the scope of future Best Practice work to identify Best Practices aimed at addressing the spread of bot malware through the network and detecting and disrupting botnet command and control traffic.

The new Best Practices are organized in areas of Prevention (12 BPs), Detection (5 BPs), Notification (2 BPs), and Mitigation (3 BPs). In addition, 2 BPs were identified in the area of Privacy Considerations concerning customer information in the context of addressing botnets.

Industry participants are strongly encouraged to have their respective subject matter experts review these Best Practices for applicability. It is critical to note that Best Practices are not applicable in every situation because of multiple factors. Therefore, these Best Practices are intended to be voluntary for the ISPs, and that mandating a particular set of practices could contribute to suboptimal network operation and reliability, or result in other negative consequences.

With this understanding, Working Group 8 recommends that the Best Practices set out in Appendix A be implemented, as applicable, by ISPs in order to address the growing botnet problem in consumer end-user devices and ISP networks.

6 APPENDIX A

CSRIC WG 8 BEST PRACTICES

Introduction to Best Practices

Best Practices are statements that describe the industry's guidance to itself for the best approach to addressing a concern. They result from unparalleled industry cooperation that engages vast expertise and considerable resources. The primary objective of Best Practices is to provide guidance from assembled industry expertise and experience. The implementation of Best Practices is intended to be voluntary. Decisions of whether or not to implement a specific Best Practice are intended to be left with the responsible organization (e.g., Service Provider, Network Operator, or Equipment Supplier). In addition, the applicability of each Best Practice for a given circumstance depends on many factors that need to be evaluated by individuals with appropriate experience and expertise in the same area addressed by the Best Practice.

The Best Practices recommended by CSRIC Working Group 8 are intended to give guidance. Decisions of whether or not to implement a specific Best Practice are intended to be left with the responsible organization (e.g., Service Provider, Network Operator, or Equipment Supplier). Mandated implementation of these Best Practices is *not* consistent with their intent. The appropriate application of these Best Practices can only be done by individuals with sufficient knowledge of company specific network infrastructure architecture to understand their implications. Although the Best Practices are written to be easily understood, their meaning is often *not* apparent to those lacking this prerequisite knowledge and experience. Appropriate application requires understanding of the Best Practice impact on systems, processes, organizations, networks, subscribers, business operations, complex cost issues and other considerations. With these important considerations regarding intended use, the industry stakeholders are concerned that government authorities may inappropriately impose these as regulations or court orders. Because these Best Practices have been developed as a result of broad industry cooperation that engages vast expertise and considerable voluntary resources, such misuse of these Best Practices may jeopardize the industry's willingness to work together to provide such guidance in the future.[4]

[4] These principles were brought forward from the work of the NRIC VII Focus Group 3B, Public Data Network Reliability Final Report, Sections 2.3.2 and 3.4.2

PREVENTION BEST PRACTICES

6.1.1 BP Number: Prevention 1

Stay Informed about Botnet/Malware Techniques:
ISPs should stay informed about the latest botnet/malware techniques so as to be prepared to detect and prevent them.

BP Reference/Comments:
See the following document for more information:
http://www.maawg.org/sites/maawg/files/news/MAAWG_Bot_Mitigation_BP_2009-07.pdf
More information can also be found at:
http://isc.sans.edu/index.html
http://www.us-cert.gov/
http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.2 BP Number: Prevention 2

ISP Provision of Educational Resources for Computer Hygiene / Safe Computing:
ISPs should provide or support third-party tutorial, educational, and self-help resources for their customers to educate them on the importance of and help them practice safe computing. ISPs' users should know to protect end user devices and networks from unauthorized access through various methods, including, but not limited to:

- Use legitimate security software that protects against viruses and spywares;
- Ensure that any software downloads or purchases are from a legitimate source;
- Use firewalls;
- Configure computer to download critical updates to both the operating system and installed applications automatically;
- Scan computer regularly for spyware and other potentially unwanted software;
- Keep all applications, application plug-ins, and operating system software current and updated and use their security features;
- Exercise caution when opening e-mail attachments;
- Be careful when downloading programs and viewing Web pages;
- Use instant messaging wisely;
- Use social networking sites safely;
- Use strong passwords;
- Never share passwords.

BP Reference/Comments:
More information can be found at:
National Cyber Security Alliance - http://www.staysafeonline.org/
OnGuard Online - http://www.onguardonline.gov/default.aspx
Department of Homeland Security -
StopBadware – http://www.stopbadware.org/home/badware_prevent
Comcast.net Security - http://security.comcast.net/
Verizon Safety & Security -
http://www.verizon.net/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_safety
Qwest Incredible Internet Security site: http://www.incredibleinternet.com/
Microsoft- http://www.microsoft.com/security/pypc.aspx

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.3 BP Number: Prevention 3

ISP Provision of Anti-Virus/Security Software:
ISPs should make available anti-virus/security software and/or services for its end-users. If the ISP does not provide the software/service directly, it should provide links to other software/services through its safe computing educational resources.

BP Reference/Comments:

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.4 BP Number: Prevention 4

Protect DNS Servers:
ISPs should protect their DNS servers from DNS spoofing attacks and take steps to ensure that compromised customer systems cannot emit spoofed traffic (and thereby participate in DNS amplification attacks). Defensive measures include:

(a) managing DNS traffic consistent with industry accepted procedures;
(b) where feasible, limiting access to recursive DNS resolvers to authorized users;
(c) blocking spoofed DNS query traffic at the border of their networks, and
(d) routinely validating the technical configuration of DNS servers by, for example, utilizing available testing tools that verify proper DNS server technical configuration.

BP Reference/Comments:
Widely accepted DNS traffic management procedures are discussed in the following document:
http://www.maawg.org/sites/maawg/files/news/MAAWG_DNS%20Port%2053V1.0_2010-06.pdf
Security issues on recursive resolvers are discussed in IETF BCP 140/ RFC 5358. Responses to spoofed traffic, including spoofed DNS traffic, are discussed in IETF BCP 38/RFC 2827.
Some tools examining different aspects of DNS server security include:

http://dnscheck.iis.se/, http://recursive.iana.org/, and https://www.dns-oarc.net/oarc/services/dnsentropy. More information on DNS security issues can also be found at: http://www.iana.org/reports/2008/cross-pollination-faq.html

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.5 BP Number: Prevention 5

Utilize DNSSEC:
ISPs should use Domain Name System (DNS) Security Extensions (DNSSEC) to protect the DNS**.** ISPs should consider, at a minimum, the following:

- sign and regularly test the validity of their own DNS zones,
- routinely validate the DNSSEC signatures of other zones;
- employ automated methods to routinely test DNSSEC-signed zones for DNSSEC signature validity.

BP Reference/Comments:
More information can be found at:
http://dnssec.net
https://www.dnssec-deployment.org

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.6 BP Number: Prevention 6

Encourage Use of Authenticated SMTP/Restrict Outbound Connections to Port 25:
ISPs should encourage users to submit email via authenticated SMTP on port 587, requiring Transport Layer Security (TLS) or other appropriate methods to protect the username and password. In addition, ISPs should restrict or otherwise control inbound and outbound connections from the network to port 25 (SMTP) of any other network, either uniformly or on a case by case basis, *e.g.*, to authorized email servers.

BP Reference/Comments:
See the following document for more information:
http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.7 BP Number: Prevention 7

Authentication of Email:
ISPs should authenticate all outbound email using DomainKeys Identified Mail (DKIM) and

Sender Policy Framework (SPF). Authentication should be checked on inbound emails; DKIM signatures should be validated and SPF policies verified.

BP Reference/Comments:
See the following document for more information:
http://www.maawg.org/sites/maawg/files/news/MAAWG_Email_Authentication_Paper_2008-07.pdf
More information can also be found at:
http://www.dkim.org/
http://openspf.org

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.8 BP Number: Prevention 8

Immediately Reject Undeliverable Email:
ISPs should configure their gateway mail servers to immediately reject undeliverable email, rather than accepting it and generating non-delivery notices (NDNs) later, in order to avoid sending NDNs to forged addresses.

BP Reference/Comments:
By rejecting undeliverable email, the gateway mail will inform the sending mail server, which can apply local policy regarding whether or not to notify the message sender of the non-delivery of the original message.
See the following document for more information:
http://www.maawg.org/sites/maawg/files/news/MAAWG-BIAC_Expansion0707.pdf

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.9 BP Number: Prevention 9

Blocking e-mail from Dynamic Space:
ISPs should not accept e-mail that originates from mail servers in dynamically-assigned IP address blocks, and should consider using one of the available services that identify such blocks.

BP Reference/Comments:

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.10 BP Number: Prevention 10

Share Dynamic Address Space Information:
ISPs should share lists of their dynamic IP addresses with operators of DNS Block Lists (DNSBLs) and other similar tools. Further, such lists should be made generally available, such as via a public website.

BP Reference/Comments:
More information can be found at:
http://www.maawg.org/sites/maawg/files/news/MAAWG_Dynamic_Space_2008-06.pdf
http://www.spamhaus.org/pbl/
http://www.mail-abuse.com/nominats_dul.html

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.11 BP Number: Prevention 11

Make Dynamic IPv4 Space Easily Identifiable by Reverse DNS Pattern:
ISPs should make IPv4 dynamic address space under their control easily identifiable by reverse DNS pattern, preferably by a right-anchor string with a suffix pattern chosen so that one may say that all reverse DNS records ending in *.some.text.example.com are those that identify dynamic space.

BP Reference/Comments:
Refer to related Best Practice Prevention 5.

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on broadband networks, but may be applicable to other users and networks as well.

6.1.12 BP Number: Prevention 12

Make Dynamic Address Space Easily Identifiable by WHOIS:
ISPs should make all dynamic address space under their control easily identifiable by WHOIS or RWHOIS lookup.

BP Reference/Comments:
See the following document for more information:
http://www.maawg.org/sites/maawg/files/news/MAAWG_Dynamic_Space_2008-06.pdf
Refer to related Best Practice Prevention 4.

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

DETECTION BEST PRACTICES

6.1.13 BP Number: Detection 1

Communicate Implementation of Situational Awareness and Protective Measures with Other ISPs:
ISPs should make reasonable efforts to communicate with other operators and security software providers, by sending and/or receiving abuse reports via manual or automated methods. These efforts could include information such as implementation of "protective measures" such as reporting abuse (e.g., spam) via feedback loops (FBLs) using standard message formats such as Abuse Reporting Format (ARF). Where feasible, ISPs should engage in efforts with other industry participants and other members of the internet ecosystem toward the goal of implementing more robust, standardized information sharing in the area of botnet detection between private sector providers.

BP Reference/Comments:
See the following document for more information:
http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf
Vulnerabilities can be reported in a standardized fashion using information provided at
http://nvd.nist.gov/
http://puck.nether.net/mailman/listinfo/nsp-security
https://ops-trust.net/
https://www2.icsalabs.com/veris/

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.14 BP Number: Detection 2

Maintain Methods to Detect Bot/Malware Infection:
ISPs should maintain methods to detect likely malware infection of customer equipment. Detection methods will vary widely due to a range of factors. Detection methods, tools, and processes may include but are not limited to: external feedback, observation of network conditions and traffic such as bandwidth and/or traffic pattern analysis, signatures, behavior techniques, and forensic monitoring of customers on a more detailed level.

BP Reference/Comments:
http://teamcymru.org
http://shadowserver.org
http://abuse.ch
http://cbl.abuseat.org

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.15 BP Number: Detection 3

Use Tiered Bot Detection Approach:
ISPs should use a tiered approach to botnet detection that first applies behavioral characteristics of user traffic (cast a wide net), and then applies more granular techniques (e.g., signature detection) to traffic flagged as a potential problem.

BP Reference/Comments:
This technique should help minimize the exposure of customer information in detecting bots by not collecting detailed information until it is reasonable to believe the customer is infected. Looking at user traffic using a "wide net" approach can include external feedback as well as other internal approaches.

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.16 BP Number: Detection 4

Do Not Block Legitimate Traffic:
ISPs should ensure that detection methods do not block legitimate traffic in the course of conducting botnet detection, and should instead employ detection methods which seek to be non-disruptive and transparent to their customers and their customers' applications.

BP Reference/Comments:

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.17 BP Number: Detection 5

Bot Detection and the Corresponding Notification Should Be Timely:
ISPs should ensure that bot detection and the corresponding notification to end users be timely, since such security problems are time-sensitive. If complex analysis is required and multiple confirmations are needed to confirm a bot is indeed present, then it is possible that the malware may cause some damage, to either the infected host or remotely targeted system (beyond the damage of the initial infection) before it can be stopped. Thus, an ISP must balance a desire to definitively confirm a malware infection, which may take an extended period of time, with the ability to predict the strong likelihood of a malware infection in a very short period of time. This 'definitive-vs.-likely' challenge is difficult and, when in doubt, ISPs should err on the side of caution by communicating a likely malware infection while taking reasonable steps to avoid false notifications.

BP Reference/Comments:

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

NOTIFICATION BEST PRACTICES

6.1.18 BP Number: Notification 1

Notification to End Users:
ISPs should develop and maintain critical notification methods to communicate with their customers that their computer and/or network has likely been infected with malware. This should include a range of options in order to accommodate a diverse group of customers and network technologies. Once an ISP has detected a likely end user security problem, steps should be undertaken to inform the Internet user that they may have a security problem. An ISP should decide the most appropriate method or methods for providing notification to their customers or internet users, and should use additional methods if the chosen method is not effective. The range of notification options may vary by the severity and/or criticality of the problem. Examples of different notification methods may include but are not limited to: email, telephone call, postal mail, instant messaging (IM), short messaging service (SMS), and web browser notification.

BP Reference/Comments:
An ISP decision on the most appropriate method or methods for providing notification to one or more of their customers or Internet users depends upon a range of factors, from the technical capabilities of the ISP, to the technical attributes of the ISP's network, cost considerations, available server resources, available organizational resources, the number of likely infected hosts detected at any given time, and the severity of any possible threats, among many other factors. The use of multiple simultaneous notification methods is reasonable for an ISP but may be difficult for a fake anti-virus purveyor.

Mitigation BP 3 provides information on how to address the malware infection.

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide services to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.19 BP Number: Notification 2

Notification Information to End Users:
ISPs should ensure that botnet notifications to subscribers convey critical service information rather than convey advertising of new services or other offers.

BP Reference/Comments:
This best practice is to help ensure that the notification message is not confused with other communications the customer may receive from the provider and help underscore the seriousness of the situation.

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide services to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

MITIGATION BEST PRACTICES

6.1.20 BP Number: Mitigation 1

Industry Cooperation During Significant Cyber Incidents:
ISPs should maintain an awareness of cyber security threat levels and, when feasible, cooperate with other organizations during significant cyber incidents, helping to gather and analyze information to characterize the attack, offer mitigation techniques, and take action to deter or defend against cyber attacks as authorized by applicable law and policy.

BP Reference/Comments:
National Cyber Incident Response Plan - The National Cyber Risk AlertLevel (NCRAL) is currently envisioned as a 4-level system in order to facilitate synchronization with several other alert level systems, such as the IT-ISAC, SANS and those from security vendors. Significant Cyber Incidents are generally labeled as Severe (level 1) and Substantial (level 2).

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.21 BP Number: Mitigation 2

Temporarily Quarantine Bot Infected Devices:
ISPs may temporarily quarantine a subscriber account or device if a compromised device is detected on the subscribers' network and the network device is actively transmitting malicious traffic. Such quarantining should normally occur only after multiple attempts to notify the customer of the problem (using varied methods) have not yielded resolution. In the event of a severe attack or where an infected host poses a significant present danger to the healthy operation of the network, then immediate quarantine may be appropriate. In any quarantine situation and depending on the severity of the attack or danger, the ISP should seek to be responsive to the needs of the customer to regain access to the network. Where feasible, the ISP may quarantine the attack or malicious traffic and leave the rest unaffected.

BP Reference/Comments:
The temporary delay of web pages for the purpose of providing web browser notification, as suggested above in the Notification Best Practices (see section 6.1.18 above), does not constitute a 'quarantine' as used in this Best Practice.
Some information regarding quarantine technology can be found at:
http://www.trustedcomputinggroup.org/developers/trusted_network_connect,

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.22 BP Number: Mitigation 3

Provide a Web Site to Assist with Malware Remediation:
ISPs should, either directly or indirectly, provide a web site to assist customers with malware remediation. Remediation of malware on a host means to remove, disable, or otherwise render a malicious bot harmless. For example, this may include but is not limited to providing a special web site with security-oriented content that is dedicated for this purpose, or suggesting a relevant and trusted third-party web site. This should be a security-oriented web site to which a user with a bot infection can be directed to for remediation. This security web site should clearly explain what malware is and the threats that it may pose. Where feasible, there should be a clear explanation of the steps that the user should take in order to attempt to clean their host, and there should be information on how users can strive to keep the host free of future infections. The security web site may also have a guided process that takes non technical users through the remediation process, on an easily understood, step-by-step basis. The site may also provide recommendations concerning free as well as for-fee remediation services so that the user understands that they have a range of options, some of which can be followed at no cost.

BP Reference/Comments:

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide services to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

PRIVACY BEST PRACTICES

6.1.23 BP Number: Privacy Considerations 1

Privacy Considerations in Botnet Detection, Notification, and Remediation:
Because technical measures to (a) detect compromised end-user devices, (b) notify end-users of the security issue, and (c) assist in addressing the security issue, may result in the collection of customer information (including possibly "personally identifiable information" and other sensitive information, as well as the content of customer communications), ISPs should ensure that all such technical measures address customers' privacy, and comply and be consistent with all applicable laws and corporate privacy policies.

BP Reference/Comments:

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

6.1.24 BP Number: Privacy Considerations 2

Measures to Protect Privacy in Botnet Response:
In designing technical measures for identification, notification, or other response to compromised end-user devices ("technical measures"), ISPs should pursue a multi-prong strategy to protect the privacy of customers' information, including but not limited to the following:

a) ISPs should design technical measures to minimize the collection of customer information;
b) In the event that customer information is determined to not be needed for the purpose of responding to security issues, the information should promptly be discarded;
c) Any access to customer information collected as a result of technical measures should at all times be limited to those persons reasonably necessary to implement the botnet-response security program of the ISP, and such individuals' access should only be permitted as needed to implement the security program;
d) In the event that temporary retention of customer information is necessary to identify the source of a malware infection, to demonstrate to the user that malicious packets are originating from their broadband connection, or for other purposes directly related to the botnet-response security program, such information should not be retained longer than reasonably necessary to implement the security program (except to the extent that law enforcement investigating or prosecuting a security situation, using appropriate procedures, has requested that the information be retained); and
e) The ISP's privacy compliance officer, or another person not involved in the execution of the security program, should verify compliance by the security program with appropriate privacy practices.

BP Reference/Comments:

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

7 APPENDIX B

CSRIC WG 8 REFERENCE LIST

REFERENCE LIST

- Alliance for Telecommunications Industry Solutions (ATIS) - http://www.atis.org/
- Anti-Botnet - http://botfrei.de
- Comcast.net Security - http://security.comcast.net/
- Composite Blocking List - http://cbl.abuseat.org
- Cyber Clean Center - https://www.ccc.go.jp/en_ccc/
- Department of Homeland Security - http://www.dhs.gov/files/programs/gc_1158611596104.shtm
- Department of Homeland Security – United States Computer Emergency Readiness Team (US-CERT) - http://www.us-cert.gov/
- DNS Check - http://dnscheck.iis.se/
- DNS Security Extensions Securing the Domain Name System (DNSSEC) - http://dnssec.net
- DNSSEC - https://www.dnssec-deployment.org
- Domain Name System Operations Analysis and Research Center (DNS-OARC) - https://www.dns-oarc.net/oarc/services/dnsentropy
- DomainKeys Identified Mail (DKIM) - http://www.dkim.org/
- International Telecommunication Union Botnet Mitigation Toolkit - http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html
- Internet Assigned Numbers Authority Cross Pollination Check - http://recursive.iana.org/
- Internet Assigned Numbers Authority FAQs on Cache Poisoning and Cross Pollination - http://www.iana.org/reports/2008/cross-pollination-faq.html
- Internet Storm Center - http://isc.sans.edu/index.html
- Messaging Anti-Abuse Working Group (MAAWG.org) – Code of Conduct - http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf
- Messaging Anti-Abuse Working Group (MAAWG.org) – Common Best Practices - http://www.maawg.org/sites/maawg/files/news/MAAWG_Bot_Mitigation_BP_2009-07.pdf
- Messaging Anti-Abuse Working Group (MAAWG.org) – Email Authentication - http://www.maawg.org/sites/maawg/files/news/MAAWG_Email_Authentication_Paper_2008-07.pdf
- Messaging Anti-Abuse Working Group (MAAWG.org) – Expansion and Clarification of the BIAC and MAAWG Best Practices for Internet Service Providers and Network Operators - http://www.maawg.org/sites/maawg/files/news/MAAWG-BIAC_Expansion0707.pdf
- Messaging Anti-Abuse Working Group (MAAWG.org) – Managing Port 25 - http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf
- Messaging Anti-Abuse Working Group (MAAWG.org) – Methods for Sharing Dynamic Address Space - http://www.maawg.org/sites/maawg/files/news/MAAWG_Dynamic_Space_2008-06.pdf
- Messaging Anti-Abuse Working Group (MAAWG.org) – Overview of DNS Security - http://www.maawg.org/sites/maawg/files/news/MAAWG_DNS%20Port%2053V1.0_2010-06.pdf
- Microsoft - http://www.microsoft.com/security/pypc.aspx
- National Cyber Security Alliance - http://www.staysafeonline.org/

- National Vulnerabilty Database – National Institute of Standards and Technology - http://nvd.nist.gov/
- NSP Security Forum (NSP-SEC) - http://puck.nether.net/mailman/listinfo/nsp-security
- OnGuard Online - http://www.onguardonline.gov/default.aspx
- OPSEC-Trust - https://ops-trust.net/
- Qwest Incredible Internet Security Site - http://www.incredibleinternet.com/
- Shadowserver Foundation - http://shadowserver.org
- Spamhaus Policy Block List - http://www.spamhaus.org/pbl/
- SPF Project - http://openspf.org
- StopBadware - http://www.stopbadware.org/home/badware_prevent
- Swiss Security Blog - http://abuse.ch
- Team Cymru Research NFP - http://teamcymru.org
- Trend Micro Maps - http://www.mail-abuse.com/nominats_dul.html
- Trusted Computing Group - http://www.trustedcomputinggroup.org/developers/trusted_network_connect
- U.S. Commerce Department's National Institute of Standards and Technology (NIST) - http://www.nist.gov/index.html
- Verizon Enterprise Risk and Incident Sharing (VERIS) - https://www2.icsalabs.com/veris/
- Verizon Safety & Security - http://www.verizon.net/central/vzc.portal?_nfpb=true&_pageLabel=vzc_help_safety