Before the

**U.S. DEPARTMENT OF COMMERCE**
National Institute of Standards and Technology
National Telecommunications and Information Administration

**U.S. DEPARTMENT OF HOMELAND SECURITY**

Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware

Docket No. 110829543-1541-01

# RESPONSE OF CENTURYLINK TO REQUEST FOR INFORMATION

## I. INTRODUCTION

CenturyLink[1] hereby responds to the Request for Information (RFI) of the U.S. Department of Commerce (DOC) and the U.S. Department of Homeland Security (DHS) (Agencies)[2] "requesting information on the requirements of, and possible approaches to creating, a voluntary industry code of conduct to address the detection, notification and mitigation of botnets."[3] CenturyLink has voluntarily undertaken a program to help curtail the spread of viruses and malicious software (malware), including botnets, and assist its customers whose computers are infected with viruses and malware. In Section II of this Response, CenturyLink

---

[1] CenturyLink is the third largest telecommunications company in the United States. CenturyLink provides broadband, voice and wireless services to consumers and businesses across the country and advanced entertainment services under the CenturyLink™ Prism™ TV and DIRECTV brands. In addition, CenturyLink provides data, voice and managed services to business, government and wholesale customers in local, national and select international markets through its high-quality advanced fiber optic network and multiple data centers. CenturyLink is also recognized as a leader in the network services market by key technology industry analyst firms, and is a global leader in cloud infrastructure and hosted IT solutions for enterprises through Savvis, a CenturyLink company. CenturyLink's customers range from Fortune 500 companies in some of the country's largest cities to families living in rural America. *See* http://www.centurylink.com/ for more information about CenturyLink.

[2] Request for Information, Federal Register, Vol. 76, No. 183, September 21, 2011, at 58466-58469. *See also* Notice; Extension of comment period, Federal Register, Vol. 76, No. 213, November 3, 2011, at 68160.

[3] RFI at 58467.

describes its Customer Internet Protection Program (CIPP). The CIPP is available to CenturyLink's residential and small business broadband customers on CenturyLink's Asymmetric Digital Subscriber Line (ADSL) network[4] and provides infection notification and assistance with the mitigation of virus and malware infections, including botnets, once such infections have been detected. CenturyLink proactively provides virus and malware notification, mitigation and security education for these broadband customers.[5] CenturyLink introduced its CIPP in 2007.[6] CenturyLink welcomes the opportunity to share with the Agencies how it detects customer virus and malware infections, notifies customers of detected infections, assists infected customers with mitigation and educates customers about practices that they can employ to best protect their computers from re-infection. CenturyLink wishes to emphasize that despite its satisfaction with the results produced by its CIPP and the favorable reception to it from CenturyLink customers, CenturyLink opposes any other ISP being required to implement the same or a similar program, or any particular element(s) of its CIPP. CIPP has worked for CenturyLink and its customers precisely because CenturyLink has been free to develop and implement, or not, an Internet protection program that is tailored to its needs and the needs of its customers.

In Section III of this Response, CenturyLink discusses its strong support for the use of public-private partnerships and voluntary best practices as viable and constructive approaches for addressing cybersecurity. CenturyLink has heavily invested in cybersecurity by employing internally developed best practices, as well as best practices developed by numerous industry

---

[4] The program is only available currently in CenturyLink's legacy Qwest local service areas. Qwest is a wholly-owned subsidiary of CenturyLink.

[5] CenturyLink also offers a portfolio of cybersecurity services to address the needs of its small and mid-size business and government customers.

[6] *See Qwest Customer Internet Protection Program Increases Security For Broadband Customers, Combats Spread Of Viruses And Malware*, http://news.centurylink.com/index.php?s=43&item=407.

organizations.[7] CenturyLink believes that ongoing public-private partnerships have proven to be effective vehicles for sharing information and developing the strategies and programs that enhance the Nation's cybersecurity posture and protect its customers. One-size-fits-all government mandates are the wrong approach for improving cybersecurity and would slow the ability of both government and the private sector to timely respond to an ever-changing cyber threat environment. Even a "voluntary code of conduct" for Internet Service Providers (ISPs) must be approached with care. If poorly done or misused, it could cause far more harm than good.

In Section IV, CenturyLink addresses the specific questions presented by the Agencies in the RFI. CenturyLink thanks the Agencies for providing this opportunity to discuss its experiences and views on this critically important matter.

## II. CENTURYLINK'S CUSTOMER INTERNET PROTECTION PROGRAM

Internet security is a top priority for CenturyLink, other ISPs and most Internet users. Viruses and malware are significant Internet security problems, and they are constantly changing. The CenturyLink CIPP is designed to help curtail the spread of viruses and malware, including botnets, on the Internet and to assist CenturyLink customers whose computers are infected with viruses or malware. The three goals of CenturyLink's CIPP are to: 1) automate the notification of virus- or malware-infected customers; 2) assist customers in an online, self-help manner to clean their computers of infections; and 3) educate its customers about the dangers of viruses and malware and benefits of good Internet security practices. CenturyLink used several general principles in designing the CIPP:

---

[7] *E.g.* Network Reliability Steering Committee of the Alliance for Telecommunications Industry Solutions (ATIS NRSC); Communications Security, Reliability and Interoperability Council (CSRIC) (a federal advisory committee under the Federal Communications Commission); Messaging Anti-Abuse Working Group (MAAWG); Internet Engineering Task Force (IETF); and National Institute of Standards and Technology (NIST).

- Assume that infected customers do not have malicious intent and are simply victims. Handle customers suspected of malicious intent with different procedures.
- Treat customers with respect.
- Warn customers of dangers to their personal information.
- Educate customers about good cybersecurity practices.
- Provide self-help tools to assist customers with cleaning their systems.

CenturyLink residential and small business broadband customers on its ADSL network automatically receive this service at no additional cost.

CenturyLink primarily relies on trusted third parties to provide information about malicious activities originating from CenturyLink customer-allocated IP addresses. These trusted third parties use a variety of techniques to identify malicious activity on the Internet. These reliable techniques include monitoring for malicious packets sent to computers or honeypots that should not be receiving traffic (also known as "dark IP monitoring"); watching for large amounts of spam sent from infected computers; monitoring for botnet command and control activity; and identifying infected computers. If CenturyLink detects a virus or malware on its network,[8] or if it is notified by a trusted third party that a customer's computer is infected, CenturyLink will notify the customer.

Upon notifying a customer of a detected infection, CenturyLink informs the customer of safe Internet security practices and offers the customer online self-help tools, if practical, to remove the infection from the computer. The customer's unencrypted World Wide Web (Web) traffic is redirected to perform the notification. Ports commonly used to spread malware are blocked while the customer is in *walled garden* status. Most normal customer e-mail is not blocked while the customer is in *walled garden* status. These customers have the option to

[8] It is important to note that CenturyLink does not actively monitor customer traffic. It will use netflow (header information but not content) if there is a need to validate information reported to it. The availability of information from trusted third parties concerning malicious activities originating from the IP addresses of CenturyLink customers is essential to the viability of the CIPP.

immediately restore their Internet connection to normal service status at this point or continue through the process for mitigation of the infection. CenturyLink asks infected customers to review the Internet security information that CenturyLink has provided and to access the downloadable or online tools that will help them remove the virus or malware. The CenturyLink CIPP home page provides customers with links to virus and malware removal guides. In some cases, customers may need to contact an anti-virus or anti-malware software provider to help them remove the virus or malware. If a customer tries to remove a virus or malware and still has problems, the customer can call CenturyLink broadband technical support; however, if the customer has a malware infection, CenturyLink encourages the customer to get assistance from an anti-malware software provider. CenturyLink does not scan customers' computers for viruses or malware nor does CenturyLink remove viruses or malware from computers for customers. Further, CenturyLink does not scan or otherwise monitor customers' content.

As noted above, CenturyLink's CIPP and its interactions with it customers are predicated on the assumption that its customers are non-malicious users of the Internet. Once notified of a suspected infection, CenturyLink customers may quickly exit *walled garden* status and their normal access to the Web is restored within minutes. CenturyLink requires infected customers to acknowledge the CIPP notification and agree to take action to address their infections. It is important to note that CenturyLink does not block CenturyLink or third-party voice over Internet protocol (VoIP) traffic, or other common, legitimate Internet protocols, while a customer is in *walled garden* status. Customers who are repeatedly notified of malicious traffic coming from their Internet account but who do not address the problem may have their broadband Internet connection disconnected pursuant to the terms of CenturyLink's Acceptable Use Policy (AUP), or they may have to call CenturyLink to have their Web access restored. This helps curtail the

spread of viruses and malware on the Internet and helps protect other CenturyLink broadband customers.

CenturyLink developed its CIPP internally. Other commercial products exist and similar systems have been used for a number of years to limit and/or prevent a user's access to Web content and services. Many of the commercial services and software programs do an excellent job of maintaining customers' Internet security, but no anti-virus/anti-spyware service or program can catch 100 percent of the infections that are circulating on the Internet. Further, malware continues to increase in sophistication. Malware writers are using more advanced technologies to avoid detection, and new types of cloaking technologies make it more difficult to detect malware. Social engineering techniques are commonly used to trick Internet users into installing malware and bypass automated controls. CenturyLink believes that its CIPP is a valuable, additional tool to help protect customers and help limit the spread of destructive viruses and malware. But, this may not be sufficient to alleviate the risk from all infections or limit the spread of all malicious viruses and malware. CenturyLink asks customers to complete a survey concerning their CIPP experience, and the survey results indicate that CIPP has been well received by its customers.

## III. CENTURYLINK SUPPORTS VOLUNTARY BEST PRACTICES

While CenturyLink believes that ISPs are in a unique position to assist in mitigating threats directed at their customers, it does not support either a mandatory ISP code of conduct or mandatory ISP best practices directed at ISP notification to consumers regarding the illicit use of computer equipment by botnets and related malware. Further, even the adoption of a voluntary code of conduct or voluntary ISP notification practices, if poorly conceived and misused, can prove to be counter-productive. Any action by the government to move from the purely

voluntary best practices model currently employed in the cybersecurity environment by ISPs must be undertaken with great care.

ISPs have a strong, direct and immediate incentive to secure their infrastructure because cyber attacks that impact service availability and the quality of customers' Internet experiences directly affect ISPs' competitive position and revenue generating opportunities. They also have an incentive to assist their customers in maximizing the benefits derived from the services provided to those customers in ways that are lawful, economically supportable and align with demonstrated customer interests. ISPs have committed, and continue to commit, significant human and financial resources to secure their own infrastructure. CenturyLink has heavily invested in cybersecurity by employing internally and industry developed best practices, including IETF standards and best current practice documents, NRIC and CSRIC cybersecurity best practices, NIST publications, International Telecommunications Union (ITU) recommendations, International Organization for Standardization (ISO) standards, and ATIS standards. In addition, CenturyLink is actively engaged in information sharing pilot programs and groups that are designed to further enhance situational awareness and responsiveness to evolving cyber conditions (*e.g.* National Security Information Exchange (NSIE); National Coordinating Center-Information Sharing and Analysis Center (NCC-ISAC)).

Specific to the matter of addressing consumer botnet infections, several industry bodies have developed, or are developing, best practices. For example, CSRIC II,[9] Working Group 8 (ISP Network Protection Practices), a federal advisory committee operating under the auspices of the Federal Communications Commission (FCC), developed ISP recommended best practices in the area of botnet/malware prevention, detection, notification and mitigation.[10] The recently

[9] Chartered March 19, 2009 to March 18, 2011.
[10] *See* ATTACHMENT hereto: APPENDIX A CSRIC WG 8 BEST PRACTICES, December 2010.

convened CSRIC III, Working Group 7 (Botnet Remediation) plans an in-depth review of: the recommendations of CSRIC II, Working Group 8; an IETF draft ISP standard on addressing consumer botnet infections; recently adopted MAAWG ISP best practices concerning detection, notification and mitigation of consumer botnet infections; and the experiences of Australia, Germany, Japan, Netherlands and Finland where ISP programs have been implemented concerning the detection and mitigation of consumer botnet infections. The review being conducted by Working Group 7 will be instrumental in assessing the most viable framework(s) for effecting concerted U.S. ISP action with respect to the detection, notification and mitigation of consumer botnet infections. While it would be imprudent to endorse the findings, conclusions or recommendations of Working Group 7 as it begins its deliberations, CenturyLink is a strong supporter of CSRIC III, generally, and the Working Group 7 process specifically. CenturyLink personnel are actively involved in CSRIC III and Working Group 7 at all levels.

In the RFI, three "scenarios" are proposed concerning possible voluntary approaches for the establishment of a centralized consumer resource center that could provide to consumers, at no cost, information and support for mitigating identified botnet infections – a private-sector run and supported resource center charged with responsibility for informing and educating consumers with infected equipment; a public/private partnership through which the government and private sector would work together to create a mechanism to inform and educate consumers with infected equipment; and a government run and supported structure to inform and educate consumers with infected equipment.[11] CenturyLink has reservations about the consumer resource center concept. CenturyLink provides its specific comments on the scenarios in Section IV, below. As a general matter, CenturyLink does not believe that ISPs should shoulder the costs of customer malware cleanup. The increasing number of Internet-connected devices in the

[11] RFI at 58468.

home, in conjunction with the increasing sophistication of malware infections, is significantly raising the cost of helping customers, and it is both unfair and untenable to require ISPs to bear this cost. An equitable and practical cost recovery model must be included in any plan to address consumer botnet and related malware infections. Should work be done to further develop the centralized consumer resource center concept, the work should be done within a broad public-private partnership framework.

## IV. PRACTICES, CONSUMER NOTIFICATION AND INCENTIVES TO NOTIFY

Below, CenturyLink responds to the specific questions presented in the RFI concerning practices to prevent, identify and mitigate botnet infections; effective consumer notification; and incentives to promote voluntary consumer notification.

*Responses To General Questions on Practices To Help Prevent and Mitigate Botnet Infections:*

### A. Effective Practices To Detect And Mitigate Botnet Infections.

The quality of the data used to trigger botnet notifications is critically important. False positive notifications can undermine an ISP's notification and mitigation program by negatively affecting customer confidence in the program, damaging ISP-customer relationships and increasing costs. CenturyLink has found that the use of verified, trusted third party sources, in conjunction with validation and verification methods (*e.g.* sampled netflow reports), has consistently produced sufficiently high quality information and allowed it to maintain an effective CIPP program. CenturyLink is aware of several broadband ISPs across the U.S., Canada and United Kingdom that use similar detection and validation/verification methods.

Notifying customers of malware infections without having an effective mitigation solution to offer to them will also negatively affect customer confidence in an ISP's program. The time between ISP infection detection and customer notification should be as short as

possible. Delays can lead to customer notifications concerning infections that have already been mitigated by customers. Also, customers often cannot obtain software updates until infections are addressed, and notification delays can leave customers exposed to additional infections.

*See* generally, CSRIC II Working Group 8 Best Practices 6.1.13-6.1.17 (Detection), 6.1.18 and 6.1.19 (Notification) and 6.1.20-6.1.22 (Mitigation).[12]

**B. Effective Preventative Measures For Stopping Botnet Infections.**

CenturyLink has found that for scan and exploit malware, Network Address Translation/Port Address Translation (NAT/PAT) and stateful firewalls[13] that allow access for all return traffic are very effective. For Web-based client-side malware, CenturyLink has found limiting privileges[14] on home computers to be the most effective preventative measure.

*See* generally, CSRIC II Working Group 8 Best Practices 6.1.1-6.1.12 (Prevention).

**C. Benefits To Promoting Voluntary Standards And Best Practices.**

CenturyLink has and continues to support truly voluntary standards and best practices. The use of voluntary best practices has proven to be successful in enhancing cybersecurity and should continue to be supported by government and industry. CenturyLink believes that there is value in ISPs working through industry groups to share successful methods on combating botnets and other malware. A voluntary code of conduct that is the result of an open process, secures broad industry-wide consensus, and that is used to inform ISPs as to what can be done rather than "shame" them into conforming to a uniform set of operations or practices could be a helpful tool. A properly structured code would allow, for instance, ISPs to share nonspecific information on successful practices through a "safe harbor" arrangement without the threat of

[12] Referenced CSRIC II Working Group 8 Best Practices are in the ATTACHMENT hereto.
[13] A type of firewall that keeps track of the state of packets that move through the firewall.
[14] Establishing non-administrative accounts on a system and using these accounts to surf the Web rather than an administrative account and thereby limiting the ability of malicious software to infect an administrative account.

liability for the use of such information.[15] A code of conduct might be relied upon, for example, to define the limits around information gathering, storage, anonymity and sharing. Any code of conduct should acknowledge that ISPs must retain the flexibility to use escalating methods that allow them to match the necessary level of network protection to the level of a given network threat.

### D. Effective Mechanisms For Sharing Information About Botnets.

The Agencies ask about existing mechanisms that could be effective in sharing information about botnets and would help prevent, detect and mitigate botnet infections.[16] CenturyLink has found that securing access to high quality, timely and validated trusted third party infected customer information is very useful. There are some very specific data attributes that must be in the information for it to be useful.[17] The dissemination mechanisms for sharing information may vary. One possibility that CenturyLink would support is sharing information through the NCC-ISAC. Most importantly, though, ISPs should not be required to pay for customer infection information.

*See* CSRIC II Working Group 8 Best Practices 6.1.13 (Detection) and 6.1.20 (Mitigation).

### E. Data That Can Be Shared By ISPs.

Timely customer infection data, as described in Subsection D above, is very useful information that could be shared by ISPs. Also, information on botnet command and control systems used to capture customer infection data could be shared to assist ISPs in validating the infected customer data, as well as details on how the infected customer data was generated in

---

[15] Such safe harbors would need to be codified so that ISPs are protected from civil and criminal legal proceedings for sharing information, as well as for notifications and mitigation performed in good faith.

[16] RFI at 58468.

[17] Including: infected_ip, time_stamp, time_zone (utc if possible), malware type if possible, malware hash values, sr_port, and dst_port if possible.

order to allow for the estimation of the false positive rate. Concerns, though, about customer sensitivities regarding information sharing, competitiveness issues, available time to assemble data and create reports, and regulations concerning the use of personally identifiable customer information present constraints on sharing information among ISPs. It is important that botnet information only be provided to the ISP or "network defense player" that has the service provider-customer relationship with the customer whose data is to be shared. In order for barriers and resistance to sharing to be lowered, policy decisions need to be made that clearly define where the legal and regulatory lines will be drawn in balancing competing privacy and malware detection/notification/mitigation interests.

### F. The Decision To Notify Upon Discovery Should Be Left To ISPs.

Decisions concerning whether and how to notify customers that they have infected devices should be left to individual ISPs. ISPs may elect not to notify customers of infections for a number reasons including a lack of confidence in the information source, the lack of timeliness in the information (stale information) and a lack of effective mitigation measures for customers. All of these issues can frustrate customers. ISPs electing to notify their customers of malware infections should be free to choose the notification method that they find most appropriate for their individual circumstances. Differences in network architecture and customer preferences may dictate a variety of notification and mitigation methods. There are industry best practices available concerning customer notification that an ISP may consider using when deciding how to notify its customers of a botnet infection.[18]

With respect to CenturyLink's CIPP, an automated support mechanism to assist the customer with mitigation of the infection is used. CenturyLink's experience indicates that the overall customer experience is better when the required customer interaction with the support

[18] *See* CSRIC II Working Group 8 Best Practices 6.1.18 and 6.1.19 (Notification).

mechanism is simple. In developing the support mechanism, assumptions concerning the computer or Internet sophistication level of the infected customer should skew toward a less sophisticated customer. For example, it may be problematic to assume that the customer can manually change the registry or delete files on an infected computer. Nonetheless, the support mechanism should be sufficiently well developed so that customers rarely require ISP intervention in order to mitigate an infection.

The support mechanism must work while the customer is infected and potentially while the customer is in a *walled garden* status. The support mechanism should take into account that many infected customers will be infected with multiple viruses or malware and have more than one device. Some form of authentication should be built into the support mechanism so that customers can trust that it is their ISP, or an authorized partner or agent of their ISP, providing the support.

### G. Support That Accommodates Customers' Preferences Is Most Effective.

In addition to the points discussed in Subsection F above, ideally a customer notification system would allow customers to select their preferred notification method in the event that their ISP detects an infected computer.[19] Short of the ideal, the more options offered to customers the better. CenturyLink believes that making more options available to customers will increase the likelihood that notifications will be timely and result in a higher level of customer confidence that ISP-generated notifications are legitimate.

### H. Scalable Measures Vary By ISP.

The Agencies ask for a description of scalable measures that parties have taken against botnets.[20] CenturyLink believes that how well a particular program will scale varies by ISP.

---

[19] *E.g.* SMS, Web redirect, tool bar application, web chat and telephone notification.
[20] RFI at 58468-69.

Differences in network architectures, notification systems, customer data integrity and other factors will all contribute to the ability of an ISP to scale a specific measure or program. CenturyLink's CIPP has proven to be scalable for its network and customer base. It is not necessarily scalable for the networks of other ISPs.

*Responses To Questions Concerning Effective Practices for Identifying Botnets:*

**I. Factors Considered By CenturyLink Concerning Customers' Privacy.**

In administering its CIPP, CenturyLink uses virus and malware detection methods that only provide it with virus and malware detection information. It examines the minimum amount of information necessary to validate virus and malware infections. CenturyLink does not ask customers to provide personal or business information. CenturyLink will ask customers to verify their user IDs. CenturyLink does not share its customers' personally identifiable information outside of CenturyLink.

*See* CSRIC II Working Group 8 Best Practices 6.1.23 and 6.1.24 (Privacy Consideration).

**J. Avoiding False Positives.**

The accuracy of malware infection information sources is very important to a successful program. Malware cleanup can be a very difficult process. The ISP or customer has to identify the infected device(s), the ISP or security provider must supply the correct tools or process to clean the infected device(s) and the customer must properly perform the mitigation process. Malicious traffic may originate from individuals piggybacking on unsecure wireless access points unknown by the legitimate broadband customer. In the future, malicious traffic may originate from TVs, blu-ray players, smartphones and appliances in the home. Some of the more advanced malware disables cleaning tools and access to Web security resources. It is possible

that some advanced malware may not be effectively removed and could require installing a new operating system, or worse, replacing the device.

As noted in Subsection D and E, above, the trust and effectiveness in any program will be directly affected by the quality and timeliness of the malware infection data sources used by an ISP. In order to minimize the number of false positives, CenturyLink validates the information that it receives concerning detected viruses and malware. It also verifies information concerning identified infections using other trusted information sources to the maximum extent possible.

### K. ISPs Are Important, But Not Exclusive, Facilitators Of The Solution.

The Agencies note that "many efforts [to date] have focused on the role of ISPs in detecting and notifying consumers about botnets."[21] They ask whether voluntary efforts in the detection and notification of botnets should only focus on ISPs.[22] CenturyLink believes that the answer is no. Operating system vendors, search engines, security software vendors and others have important roles to play in the continuum of botnet (and malware generally) prevention, detection, notification and mitigation. An effective, broadbased campaign against malware will require the cooperation of all of these stakeholders. CenturyLink has at various times engaged in cooperative efforts with these entities and believes that there is an opportunity, and need, to bring them into the policy discussion about combating viruses and malware, including botnets. There is a compelling need for a multi-layered approach to the problem of consumer infections. At a minimum, all commercial entities that are integral to the operation of the Internet have an opportunity to reinforce a culture of cyber-hygiene. There should be coordination in the delivery of messages to consumers in order to avoid confusing and duplicative messages.

*Responses To Questions Concerning Effectiveness of Consumer Notification:*

---

[21] *Id.* at 58469.
[22] *Id.*

### L. Baselines Available For Understanding The Spread And Impacts Of Botnets.

Reports have been published by companies such as Shadowserver,[23] Arbor Networks[24] and McAfee[25] that analyze the spread and negative impacts of botnets and related malware. The Conficker Working Group has also produced a report with informative data.[26] CSRIC II, Working Group 8 received reports from Neustar, the Spamhaus Project, Damballa, MAAWG and the National Cyber Security Alliance on their respective findings, recommendations and insights into botnet prevention, detection, notification and mitigation that should be helpful to the agencies.[27]

### M. How To Notify Upon Discovery Of Botnets Should Be Left To ISPs.

See the points discussed and citations referenced in Subsections F and G above.

### N. Standard Elements For Inclusion In Notices May Be Appropriate.

Notices and the process by which they are delivered should not be mandated. If an ISP chooses to notify its infected customers, it should have the flexibility to design a notice that is appropriate for its individual situation. It may be reasonable, though, for a voluntary best practice to be developed that would identify the elements that are recommended to be contained

---

[23] *See* http://www.shadowserver.org/wiki/pmwiki.php/information/botnets.
[24] *See* lhttp://www.arbornetworks.com/arbor-networks'-sixth-annual-worldwide-infrastructure-security-report.htm.
[25] *See* http://www.mcafee.com/us/about/news/2011/q2/20110601-01.aspx.
[26] *See* http://www.confickerworkinggroup.org/wiki/#toc1.
[27] *See* Spamhaus Policy Block List - http://www.spamhaus.org/pbl/; MAAWG – Code of Conduct - http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf; MAAWG – Common Best Practices - http://www.maawg.org/sites/maawg/files/news/MAAWG_Bot_Mitigation_BP_2009-07.pdf; MAAWG – Email Authentication - http://www.maawg.org/sites/maawg/files/news/MAAWG_Email_Authentication_Paper_2008-07.pdf; MAAWG – 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; MAAWG – Managing Port 25 - http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf; MAAWG – Methods for Sharing Dynamic Address Space - http://www.maawg.org/sites/maawg/files/news/MAAWG_Dynamic_Space_2008-06.pdf; MAAWG – Overview of DNS Security - http://www.maawg.org/sites/maawg/files/news/MAAWG_DNS%20Port%2053V1.0_2010-06.pdf; National Cyber Security Alliance - http://www.staysafeonline.org/. *See also* http://www.damballa.com/ and http://www.neustar.biz/.

in notices to infected customers.[28] Given the creativity and motivation of cyber criminals, a standard notice alone may diminish but not eliminate the possibility of fraudulent notifications.

Based on its experience, CenturyLink believes that a secondary, out-of-band verification process could be considered that would increase customer trust in the ISP's notification. Such a system may be costly and should not be mandated. Infected CenturyLink CIPP customers that encounter problems with mitigation or have questions about the notifications that have been received are able to contact the CenturyLink Help Desk. The Help Desk customer representative is automatically alerted that the customer is in a *walled garden* status and has been notified of an infection. CenturyLink's experience thus far is that the number of customers contacting its Help Desk has not been significant enough to create cost concerns.

### O. ISP's Should Be Free To Determine The Most Effective Pricing For Mitigation Services.

As noted in Section II, above, CenturyLink's CIPP is provided to customers free of charge and the use of a *walled garden* provides an incentive for customers to respond to notifications that they have an infected device. CIPP has been well received by customers, and CenturyLink continues to find it cost-effective. Once infection mitigation has occurred, most customers are more aware of the risks that use of the Internet presents, and they exercise greater care.

CenturyLink has limited data on the attractiveness of free versus for-fee products to customers and the effectiveness of free services without other inducements in both cleaning computers and preventing re-infections. Costs affect the resources that an entity can commit to mitigation services. Paid services are generally more robust and comprehensive in nature.

[28] CSRIC III, Working Group 7 will, as part of its Charter, review foreign approaches to notifications which may provide a basis for a recommendation or best practice on standardized notifications.

CenturyLink believes that ISPs should be free to determine the most effective pricing model for their mitigation services.

**P. Data Is Insufficient To Assess The Impact Of A Consumer Resource Center.**

CenturyLink has no data or experiences that would allow it to provide an informed judgment about the impact of a consumer resource center, as described in the RFI, on value-added security services. A consumer resource center could be used to provide a trusted, out of band verification for customer infection notifications. That such a consumer resource center, or a similar entity, has not emerged to date suggests that there may be insufficient market demand for the services it would offer. If a consumer resource center were to be created, the costs to develop and support it should not be borne by ISPs.

**Q. Addressing Non-Responsive Customers.**

As discussed in Section II above, CenturyLink places customers in a *walled garden* status and denies certain access to the Web upon notification to customers of a detected infection. Customers are able to quickly restore normal Web access. Customers that delay in responding are provided additional notifications. A small percentage of the customers notified of an infection never respond or take action to mitigate the infection. CenturyLink reserves the right to disconnect the broadband Internet connection of these customers when their actions or inaction constitute a violation of CenturyLink's AUP.

CenturyLink believes that it is ultimately up to the ISP to determine the next steps when a customer is unresponsive to notifications and requests to mitigate an infection. It would be helpful if a consistent escalation model were to be developed that all ISPs providing notifications could use. The model should not advantage or disadvantage an ISP that uses it. A consistent

escalation model that all ISPs use and is communicated to consumers would level the competitive playing field for ISPs.

### R. Foreign Codes Of Conduct And Mitigation Techniques.

The Agencies ask about the effectiveness of and lessons learned from foreign codes of conduct such as those developed by Japan, Germany and Australia.[29] CenturyLink has insufficient data to assess the effectiveness of foreign ISP codes of conduct and mitigation techniques. U.S. ISPs and policymakers will know more about the lessons, if any, to be learned from these foreign ISP codes of conduct after CSRIC III Working Group 7 completes its review of the codes of conduct and associated mitigation techniques.[30]

### S. Measuring The Effectiveness Of Notices/Messages To Customers.

MAAWG is considering best practices to measure the effectiveness of infection notification and educational messages. These metrics can be difficult to measure. Additional work is needed in order to standardize methods for assessing the effectiveness of ISPs' notification and remediation efforts. In the course of evaluating the effectiveness of ISPs' notification and remediation efforts, it is very important that data attributable to specific ISPs be kept confidential and only shared in an aggregated, anonymous form. Exit surveys of CenturyLink's CIPP customers have helped CenturyLink improve its *walled garden.*

*Responses To Questions Concerning Incentives To Promote Voluntary Consumer Notification:*

---

[29] RFI at 58469.

[30] The CSRIC III Charter, as it pertains to Working Group 7, states in part: "This Working Group will review the efforts undertaken within the international community, such as the Australian Internet Industry Code of Practice, and among domestic stakeholder groups, such as IETF and the Messaging Anti-Abuse Working Group, for applicability to U.S. ISPs. Building on the work of CSRIC II Working Group 8 ISP Network Protection Practices, the Botnet Remediation Working Group shall propose a set of agreed-upon voluntary practices that would constitute the framework for an opt-in implementation model for ISPs. The Working Group will propose a method for ISPs to express their intent to opt-into the framework proposed by the Working Group."

### T. Liability Protection For Notices To Customers Of Device Infections.

ISPs should receive liability protection for notifying their customers that their devices have been infected by botnets. A safe harbor should be established which insulates ISPs from legal exposure to the extent that their notices to customers concerning device infections fall within the bounds of the conduct that defines the safe harbor. The safe harbor should encompass notifications sent in good faith. To augment the safe harbor, there should be an education campaign undertaken to sensitize the public to the benefits of ISPs engaging in infection notification and mitigation efforts. Also see the points discussed in Subsection C above.

### U. Effectiveness In Assisting Customers With Device Mitigation.

Most ISPs that provide infection notifications to their customers also provide some level of mitigation assistance. CenturyLink has found that infection mitigation effectiveness varies by the type of malware infecting a customer's computer.[31] Some malware blocks customers from going to well-known anti-virus and operating system vendor websites. ISPs may have to locally host tools to enable their customers to access remediation programs and tools. Also see the points discussed in Subsection J above.

*See* CSRIC II Working Group 8 Best Practice 6.1.22 (Mitigation).

### V. A Private Sector Approach Does Not Require A New Entity.

As noted in Section III and Subsection P above, CenturyLink has reservations concerning the consumer resource center concept. If a consumer resource center were to be created employing the private sector approach, CenturyLink does not believe that a new entity would be needed to run the project. Much of what is envisioned to be done by a consumer resource center is already being done on a decentralized basis in the private sector. Funding for the work already

[31] For example, CenturyLink has experienced a higher effectiveness rate (customers not re-infected) with respect to botnet mitigation in the CIPP. The effectiveness rate for other infections falls within a wide range.

being done would likely be welcomed. Entities that could take a leadership role include CSRIC, IETF, Ops-trust,[32] NSP-Security[33] and the Global Infrastructure Alliance for Internet Safety (GIAIS).[34]

### W. Government's Role In A Public-Private Partnership Model.

If a consumer resource center were to be created employing the public-private partnership approach, government should be the funding source for the project. From among a pool of public and private sector experts already working in this area, a committee of experts should be chosen to make decisions and direct the operations of the consumer resource center. Active stakeholders should include IETF, Ops-trust, NSP-SEC and GIAIS. Government agencies with technical resources already engaged in this area should participate. Government agencies could best contribute resources by providing more law enforcement officers to work the cases provided by the private sector.

### X. A Government-Run Approach Is Ill-Advised.

CenturyLink believes that a government-run approach is not viable, and it is ill-advised. If a consumer resource center were to be created employing the government-run approach, US-CERT, DHS and CSRIC should play leading roles.

## V. CONCLUSION

CenturyLink has implemented a program for the prevention, detection, notification and mitigation of malicious consumer device infections (viruses and malware, including botnets) that is, for CenturyLink, cost effective and helpful for itself and its customers. CenturyLink was able to do so because it was free of any government mandates to create a program incorporating particular processes or operational attributes. CenturyLink believes that no ISP should be

---

[32] *See* https://ops-trust.net/.
[33] *See* http://puck.nether.net/mailman/listinfo/nsp-security.
[34] *See* https://www.microsoft.com/presspass/press/2004/feb04/02-24giaispr.mspx.

required to adopt a particular program for the prevention, detection, notification or mitigation of consumer device infections or the particular elements of a program.

CenturyLink does not support a mandatory ISP code of conduct or best practices governing notifications to consumers concerning device infections. As pointed out in Section IV, Subsection F, of this Response, there are many legitimate reasons why an ISP would not adopt a consumer device infection notification program. Any voluntary ISP code of conduct or best practices concerning consumer notification must be developed within a broad public-private partnership framework and be widely supported by ISPs. ISPs should not be required to bear the costs of a notification program. An equitable and practical cost recovery model that takes into account the shared responsibility of all stakeholders involved in Internet commerce for a healthy Internet environment should be addressed in any ISP code of conduct or best practice concerning notification to consumers of device infections.

Respectfully submitted,

**CENTURYLINK**

By: /s/ Lawrence E. Sarjeant

Lawrence E. Sarjeant
1099 New York Avenue, N.W.
Suite 250
Washington, DC 20001
202-429-3112
Lawrence.sarjeant@centurylink.com

Its Attorney

November 14, 2011

# ATTACHMENT


December 2010

# FINAL REPORT

# Internet Service Provider (ISP) Network Protection Practices

## Working Group 8

# 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.