CSRIC III
Communications Security, Reliability and Interoperability Council

March 2012

Final Report

U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)

(A Voluntary Code)

"This Code of Conduct would be a major step forward and a significant complement to the Administration's broader efforts against botnets."

FCC Chairman Julius Genachowski
February 22, 2012

WORKING GROUP 7 - Botnet Remediation

Table of Contents

1 Results in Brief

1.1 Executive Summary

A malicious "bot" refers to a program that is installed on a system in order to enable that system to automatically perform a task, or set of tasks, typically under the command and control of a nefarious remote administrator. The growth of bot infected end-user devices[1] represents a meaningful threat to the vitality and resiliency of the Internet and to the online economy. Botnets are networks of Internet-connected end-user computing devices infected with bot malware, which are remotely controlled by third parties for nefarious purposes. Bots and botnets can lead to theft of personal information, attacks against public and private networks, and exploitation of end-users' computing power and Internet access.

The CSRIC III tasked Working Group 7, Botnet Remediation, with proposing a set of agreed-upon voluntary practices that would constitute the framework for an opt-in implementation model for ISPs to follow to mitigate the botnet threat. In response, the U.S. Anti-Bot Code of Conduct for ISPs was developed to address the threat of bots and botnets in residential broadband networks through voluntary participation. It was determined in developing the Code that constituents of the entire Internet ecosystem have important roles to play in addressing the botnet threat and that ISPs depend on support from the other parts in the ecosystem.

The Code encourages ISPs to participate in activities in support of end-user education to prevent bot infections, detection of bots, notification of potential bot infections, remediation of bots, and collaboration and sharing of information from participating in the Code. The Code is included in the Appendix.

The Working Group proposed a set of agreed upon voluntary practices that would constitute the framework for an opt-in implementation model for ISPs to help address the botnet threat. The Working Group recommends actions that ISPs offering residential broadband Internet access may take if they choose to adopt the Code. The Working Group further recommends ISPs and other service providers indicate their agreement to participate in the voluntary Code by contacting the industry organization ultimately administering participation in the Code. Initially it is suggested that participating ISPs and other service providers either notify the entity of their own choice regarding their code participation or self assert on their own web site. Future work identified includes determining the long term administration of Code participation, periodic updates to the Code, identifying barriers to Code participation, defining metrics, and identifying best practices and lessons learned among Code participants and supporting ecosystem contributors.

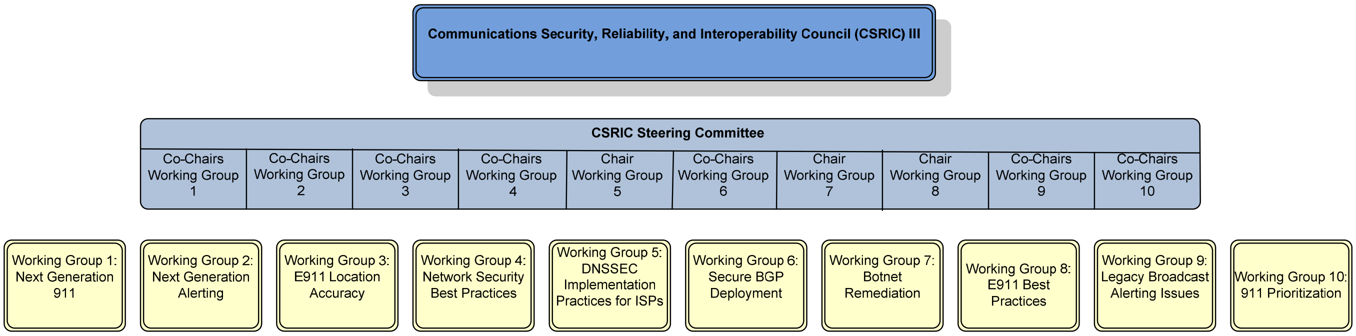
[1] The terms bot and bot infection are used interchangeably in this document.

2 Introduction

CSRIC III established Working Group 7 (WG7) to address botnet remediation in broadband networks. WG7 investigated work on bot remediation that is taking place in the IETF, Japan, Australia, Finland, Germany, and elsewhere to determine the best approach to address the bot threat in United States' broadband networks.

The result of this work is the voluntary U.S. Anti-Bot Code of Conduct for Internet Service Providers which can be found in the Appendix.

2.1 CSRIC Structure


Communications Security, Reliability, and Interoperability Council (CSRIC) III
CSRIC Steering Committee
Co-Chairs Working Group 1
Co-Chairs Working Group 2
Co-Chairs Working Group 3
Co-Chairs Working Group 4
Chair Working Group 5
Co-Chairs Working Group 6
Chair Working Group 7
Chair Working Group 8
Co-Chairs Working Group 9
Co-Chairs Working Group 10
Working Group 1: Next Generation 911
Working Group 2: Next Generation Alerting
Working Group 3: E911 Location Accuracy
Working Group 4: Network Security Best Practices
Working Group 5: DNSSEC Implementation Practices for ISPs
Working Group 6: Secure BGP Deployment
Working Group 7: Botnet Remediation
Working Group 8: E911 Best Practices
Working Group 9: Legacy Broadcast Alerting Issues
Working Group 10: 911 Prioritization

2.2 CSRIC WG7 Structure

WG7 is chaired by Michael O'Reirdan, Chairman of the Messaging Anti-Abuse Working Group (MAAWG), and vice-chaired by Dr. Peter Fonash, Chief Technology Officer, Office of Cybersecurity and Communications, Department of Homeland Security. Members of WG7 include representatives from ISPs, suppliers of software and network equipment, academia, as well as other organizations that are a part of the Internet ecosystem.

2.3 Working Group 7 Team Members

Working Group 7 consists of the members listed below.

Name	Company
Michael O'Reirdan – Chair	MAAWG
Peter Fonash – Vice-Chair	Department of Homeland Security
Neil Schwartzman - Secretary	CAUCE
Robert Thornberry - Editor	Bell Labs, Alcatel-Lucent
Paul Diamond - Editor	CenturyLink
Vernon Mosley – Liaison	FCC
Alex Bobotek	AT&T
Adam O’Donnell	Sourcefire
Alfred Huger	Sourcefire
Barry Greene	ISC
Bill McInnis	IID
Bill Smith	PayPal
Brian Done	Department of Homeland Security
Chris Roosenraad	Time Warner Cable
Chris Sills	IID
Craig Spiezle	Online Trust Alliance (OTA)
Daniel Bright	EMC
Eric Osterweil	Verisign
Gabe Iovino	REN-ISAC
Greg Holzapfel	Sprint
Gunter Ollmann	Damballa
James Holgerson	Sprint
Jay Opperman	Comcast
Joe St Sauver	University of Oregon and Internet2
Johannes Ullrich	SANS Institute
John Denning	Bank of America
John Griffin	Telecommunication Systems Inc.
John St. Clair	Verizon
Jon Boyens	National Institute of Standards and Technology
Kevin Sullivan	Microsoft
Kurian Jacob	FCC
Matt Carothers	Cox
Maxim Weinstein	StopBadware
Merike Kaeo	ISC
Michael Fiumano	Sprint
Michael Glenn	CenturyLink
Robert Mayer	USTelecom
Tice Morgan	T-Mobile
Tim Rohrbaugh	Intersections
Timothy Vogel	Verizon

Table 1 - List of Working Group 7 Members

3 Objective, Scope, and Methodology

3.1 Objective

The CSRIC tasked Working Group 7, Botnet Remediation, with proposing a set of agreed-upon voluntary practices that would constitute the framework for an opt-in implementation model for ISPs to follow in order to mitigate the botnet threat. In response, the U.S. Anti-Bot Code of Conduct for ISPs was developed to address the threat of bots and botnets in residential broadband networks through voluntary participation.

3.2 Scope

This section identifies the problem statement, working group description, and deliverables outlined in the CSRIC III charter for Working Group 7.

Problem Statement: The growth of bot infected end-user devices[2] represents a meaningful threat to the vitality and resiliency of the Internet and to the online economy. Botnets are networks of Internet-connected end-user computing devices infected with bot malware, which are remotely controlled by third parties for nefarious purposes. Bots and botnets can lead to theft of personal information, attacks against public and private networks, and exploitation of end-users' computing power and Internet access.

In order to reduce the bot infections in residential end-user devices and mitigate the potential exploitation of the bots, the voluntary U.S. Anti-Bot Code of Conduct for ISPs was developed by the Working Group 7 members.

Working Group 7 Description: 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 op-into the framework proposed by the Working Group. The Working Group will also identify potential ISP implementation barriers to the newly drafted Code and identify steps the FCC can take that may help overcome these barriers. Finally, the Working Group shall identify performance metrics to evaluate the effectiveness of the Code at curbing the spread of bot infections.

[2] The terms bot and bot infection are used interchangeably in this document.

<u>Report Deliverables</u>:

1. U.S. Anti-Bot Code of Conduct for ISPs: March 22, 2012
2. Barriers to Code Participation: September 12, 2012
3. Bot Remediation Performance Metrics: December 5, 2012

This report, the U.S. Anti-Bot Code of Conduct for ISPs, is the first of three report deliverables for the Working Group 7.

3.3 Methodology

Working Group 7 began its research into the development of a voluntary U.S. Anti-Bot Code of Conduct for ISPs by assembling a team of experts from industry, government, and academia, representing diverse stakeholders in the development and implementation of the Code. The Working Group 7 reviewed the efforts undertaken within the international community, including the Australian Internet Industry Code of Practice and the Japanese Cyber Clean Center, and among domestic stakeholder groups, including the Internet Engineering Task Force (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 CSRIC III Working Group 7 established biweekly conference calls amongst its members to discuss the development, content, and relevancy of related efforts towards the establishment of a U.S. Anti-Bot Code of Conduct for ISPs. The Working Group 7 coordinated its Code development efforts with the Department of Commerce and the National Security Staff of the White House through regular conference calls to discuss areas of mutual botnet remediation interests. The Working Group 7 held two face-to-face meetings with its members, one in November 2011 to develop the structure and discuss the content of sections of the draft Code, and a final face-to-face meeting in February 2012 to review the draft final Code. The resulting U.S. Anti-Bot Code of Conduct for ISPs is based on the collective input of the Working Group 7 members, and discussions those members and their companies have had with other stakeholders in reducing the incidence of bot infections.

4 Background[3]

A malicious or potentially malicious "bot" refers to a program that is installed on a system in order to enable that system to automatically (or semi-automatically) perform a task or set of tasks typically under the command and control of a nefarious remote administrator, or "bot master." Bots are also known as "zombies." Such bots may have been installed surreptitiously, without the user's full understanding of what the bot will do once installed, unknowingly as part of another software installation, under false pretenses, or in a variety of other possible ways.

Devices used by Internet users can be infected with malware that may contain or install one or more bots on a device. They can present a major problem for a number of reasons. First, these bots can be used to send spam, in some cases very large volumes of spam. This spam can result in extra cost for the ISPs in terms of wasted network, server, or personnel resources, among

[3] See Recommendations for the Remediation of Bots in ISP Networks, http://tools.ietf.org/rfc/rfc6561.txt

many other potential costs and side effects. Such spam can also negatively affect the reputation of the ISP, their customers, and the email reputation of the IP address space used by the ISP (often referred to simply as 'IP reputation').

In addition, these bots can act as platforms for directing, participating in, or otherwise conducting attacks on critical Internet infrastructure. Bots are frequently used as part of coordinated Distributed Denial of Service (DDoS) attacks for criminal, political, or other motivations.

The role of ISPs in providing services to Internet users, places ISPs in position to be able to attempt to detect and observe botnets operating in their networks. Furthermore, ISPs may also be in a position to be able to notify their customers of actual, potential, or likely infection by bots.

From end-users' perspectives, being notified that they may have an infected device on their network provides important information. Once they know this, they can take steps to remove the bots, resolve any problems which may stem from the bot infection, and protect themselves against future threats.

Working Group 7 developed the voluntary U.S. Anti-Bot Code of Conduct for ISPs to address the threat of bots and botnets, described above, in residential broadband networks. Adoption of the Code by ISPs is voluntary. It is not mandatory.

5 Recommendations

5.1 Recommendations

The Working Group proposed a set of agreed upon voluntary practices that would constitute the framework for an opt-in implementation model for ISPs to help address the botnet threat. The Working Group recommends actions that ISPs offering residential broadband Internet access may take if they choose to adopt the Code. The Working Group further recommends ISPs and other service providers indicate their agreement to participate in the voluntary Code by contacting the industry organization ultimately administering participation in the Code. As a voluntary Code of Conduct developed by the industry, and for the industry, the goal is for a neutral industry forum to receive and collate reports relating to participation in the Code. Initially to indicate participation, it is suggested that participating ISPs and other service providers either notify the entity of their own choice regarding their Code participation or self assert on their own web site.

5.1.1 Future Work

This report, the voluntary U.S. Anti-Bot Code of Conduct for ISPs, is the first of three report deliverables for Working Group 7. Work remains to address the long-term administration of the Code and periodic updates. Next, the Working Group will identify potential barriers to Code participation. As a final step, the Working Group will identify potential bot remediation performance metrics.

Future work is recommended to address bot infection delivery mechanisms from infected and nefarious websites and hosting services in order that the efforts of WG7 become ubiquitous, and thus effective.

5.1.2 Acknowledgements

WG7 wishes to thank Yurie Ito from the Japan CERT for her informative presentation and discussion of lessons learned from the Japan Cyber Clean Center, Japan's anti-botnet program. We also thank Ari Schwartz from National Institute of Standards (NIST) for his presentation on the botnet threat and mitigation strategies. Also, WG7 thanks Microsoft, MAAWG, and the FCC for hosting face-to-face WG7 meetings.

WG 7 would particularly like to thank the following members of the group whose unstinting efforts have contributed massively to the Code development process:

Robert Thornberry, of Bell Labs, Alcatel-Lucent (Editor)
Paul Diamond, CenturyLink (Editor)
Joe St Sauver, University of Oregon and Internet2 (Glossary)
Neil Schwartzman, CAUCE (Secretary)

6 Conclusions

In response to the CSRIC III tasking to the Working Group 7, the voluntary U.S. Anti-Bot Code of Conduct for ISPs was developed to address the threat of bots and botnets in residential broadband networks through voluntary participation. It was determined in developing the Code that constituents of the entire Internet ecosystem have important roles to play in addressing the botnet threat and that ISPs depend on support from the other parts in the ecosystem.

This March 22, 2012 report, the U.S. Anti-Bot Code of Conduct for ISPs, is the first of three report deliverables for the Working Group 7. Next, the Working Group will identify potential barriers to Code participation, with a report forthcoming in September 2012. As a final step, the Working Group will identify botnet remediation performance metrics and submit its report on this topic in December 2012.

7 Appendix

U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs)
Addressing Bot Activity in Broadband Networks
Final
March 22, 2012

1. Introduction

The growth of bot* infected end-user* devices represents a meaningful threat to the vitality and resiliency of the Internet and to the online economy. Note that bot infection and bot are used synonymously in this document to refer to an end-user device infected with bot malware. Botnets are networks of Internet-connected end-user computing devices infected with bot malware*, which are remotely controlled by third parties for nefarious purposes.

Bots and botnets can lead to theft of personal information, attacks against public and private networks, and exploitation of end-users'* computing power and Internet access. Public awareness of bots, their impact, and the resulting security and privacy issues is low. This voluntary code of conduct ("Code") provides a set of principles and recommended activities that Internet Service Providers may adopt to help address the threats presented by the presence of bots and botnets in residential broadband networks.

It should be recognized that bots impact the entire Internet ecosystem* and that successfully curtailing bots or mitigating their impact will require collective action by all parts of that ecosystem, including end-users, software developers, search providers, websites, e-commerce sites, and others. End-user devices are outside of the control of ISPs* hence all participants in the Internet ecosystem need to work together to address this issue. This Code seeks to lay the groundwork for future coordination among various stakeholders by defining a set of actions appropriately directed to the limited role ISPs can play to help address this important issue. The Code recognizes the substantial variability in size, resources, business models and environments, expertise, and abilities of the ISPs in the United States. The success of ISP activities relies on similar efforts by other Internet stakeholders.

The core requirements for participation in this Code are set forth in Section 5. The other sections of this document contain background information or additional explanatory material.

[*] Definition found in Glossary

2. Definitions of Key Terms

Note to the Reader:

Any discussion of bots inevitably involves a unique technical vocabulary. Recognizing that many readers may not be familiar with some of those specialized terms, the Code includes a glossary as Appendix 2. Any term appearing in the glossary will be marked with an asterisk "*" in the body of the Code text the first time it appears as a way of alerting the reader that a definition is available in the glossary.

3. Objectives and Principles

a. The objectives of this Code are to:

1. Provide an initial framework for ISPs to better understand and help address the bot issue; and

2. Encourage ISPs to

• Educate end-users of the threat posed by bots and of actions end-users can take to help prevent bot infections;

• Detect bot activities or obtain information, including from credible third parties, on bot infections among their end-user base;

• Notify end-users of suspected bot infections or help enable end-users to determine if they are potentially infected by bots; and

• Provide information and resources, directly or by reference to other sources, to end-users to assist them in remediating bot infections.

b. Implementation of the Code will be guided by the following principles:

1. Voluntary — participation is voluntary and encourages types of actions to be taken by ISPs, however this Code does not require any particular activity.

2. Technology neutral — this Code does not prescribe any particular means or methods.

3. Approach neutrality — this Code does not prescribe any particular approach to implement any part of this Code.

4. Respect for privacy — ISPs must address privacy issues in an appropriate manner consistent with applicable laws.

5. Legal compliance — activities must comply with applicable law.

6. Shared responsibility — ISPs, acting alone, cannot fully address the threat posed by bots. Other Internet ecosystem participants must also do their part.

7. Sustainability — ISPs should seek activities that are cost-effective and sustainable within the context of their business models.

8. Information sharing — ISPs should indicate how they are participating in the Code and share lessons-learned from their activities with other appropriate stakeholders. All information sharing between ISPs and other involved parties must be performed in accordance with applicable laws including, but not limited to, antitrust and privacy laws.

9. Effectiveness — ISPs should be encouraged to engage in activities that have been demonstrated to be appropriate and effective.

10. Effective Communication — Communication with customers* should take into account various issues such as language and make sure that information is provided in a manner that is reasonably expected to be understood and accessible by the recipients.

4. Scope and Roles

This Code was drafted specifically for ISPs and other service providers offering broadband Internet access service to residential end-users. The activities in this Code may be adapted for use by other Internet providers and participants.

This Code is not meant to be an all-inclusive approach to online security, but is meant to coexist with other current and future efforts. It anticipates a significant role for other Internet ecosystem participants, including but not limited to:

- Security software vendors
- Operating system developers
- End-user focused organizations
- Providers of Internet content, applications, and services

Online security should include a multifaceted, flexible approach using advice and tools from various reputable sources.

a. Definition of Success

Initial success of this Code will be assessed in terms of participation by the ISP community. Support by the Internet ecosystem at large, however, is seen as paramount to the ultimate success in the fight against bots.

b. Benefits of Participation in the Code

The following high-level benefits may result from meaningful ISP participation in this Code:

- Increased security of end-user information and devices and for U.S. infrastructure;

- Increased awareness of the bot threat and how to address it among end-users, ISPs, and other Internet-related industry participants;

* Definition found in Glossary

- Notification[*] and remediation[*] of bot activity on bot infected end-user devices;

- Creation of an environment in U.S. residential broadband networks that is even more hostile to the deployment and utilization of bots; and

- Development and wider use of effective notification and remediation architectures and tools across end-users and ISPs.

Some ISPs participating in the Code development process who have previously implemented some aspects of the Code have experienced beneficial results in areas such as lower call volumes to help desks from customers with infected machines, reduced upstream bandwidth consumption by denial-of-service attacks and spam[*], increased customer goodwill and lower customer churn, and reduction in spam-related complaints from other ISPs. Although individual results may vary, ISPs are encouraged to look for specific ways in which Code participation bolsters their overall broadband business, and to share those experiences with other ISPs. In addition, ISP participation in this Code may enable ISPs to generate tangible metrics relating to the impact of specific activities on the ISPs overall broadband business operations, which in turn may support development or deployment of further anti-bot activities.

[*] Definition found in Glossary

5. Parameters for Participation

Participation in this Code is voluntary.

Voluntary Code of Conduct Participation Requirements

To participate in this Code, an ISP will engage in at least one activity (i.e., take meaningful action) in each of the following general areas:

- Education - an activity intended to help increase end-user education and awareness of botnet issues and how to help prevent bot infections;
- Detection - an activity intended to identify botnet activity in the ISP's network, obtain information on botnet activity in the ISP's network, or enable end-users to self-determine potential bot infections on their end-user devices;
- Notification - an activity intended to notify customers of suspected bot infections or enable customers to determine if they may be infected by a bot;
- Remediation - an activity intended to provide information to end-users about how they can remediate bot infections, or to assist end-users in remediating bot infections.
- Collaboration - an activity to share with other ISPs feedback and experience learned from the participating ISP's Code activities.

The concept of engaging in "at least one activity" in each of these general areas is intended to encourage some level of activity in each of the five areas noted above as part of an overall nationwide process of creating an environment in U.S. residential broadband networks that is even more hostile to the deployment and utilization of bots. It is intended to support and encourage a wide range of flexible efforts to experiment and innovate with various methods of education, detection*, notification, and remediation. In that same vein, the requirement to share feedback with other ISPs is not intended to dictate any specific means or methods of sharing such feedback.

* Definition found in Glossary

6. End-User Education

a. Overview

End-users are ultimately responsible for protection of their devices and for remediating an infected device. ISPs, like many other Internet participants and government actors, can assist in helping to educate end-users about the threats presented by bots and the steps end-users can take to protect their devices and remediate infections.

b. Recommended Action:

1. Education about bot prevention[*]:

   ISPs should make available information about the prevention of bot infections and related issues. At a minimum, such information should include:

   - How and why end-users must keep their software updated for computers and devices with readily available software updates.

   - The importance of using effective and current security software from a reputable vendor.

   - The importance of backing up user data and software and how to do it effectively.

   - Basic end-user actions for minimizing exposure to bot infections while using the Internet.

   It is expected that many ISPs will be able to accomplish this goal by providing this information directly to their subscribers or by linking to existing, publicly-available sources of such information.

2. Support of end-user bot remediation efforts:

   Along with information on prevention, ISPs should make available (e.g., via ISP publications, third-party publications or web links) information on how end-users can generally remediate bot infections. In this area, it is expected that ISPs will be able to accomplish this goal by linking to existing, publicly available sources of such information or by creating new sources of such information, either individually or in conjunction with others.

   In connection with an ISP’s end-user notification activities, ISPs should include in such notices or otherwise, information on where the recipient might turn for additional information and assistance. Such information might include links to publicly-available online information, security tools, or suggestions to seek assistance of a computer professional. Additional subjects and references that an ISP might wish to include are:

[*] Definition found in Glossary

- Risks to the end-user and Internet community from using a device that is believed to be infected,
- How to identify and remove common forms of bot infections,
- Publicly-available tools or services (free or paid) to assist in the detection and removal of bot infections, and
- Guidance on where to find additional (free or paid) assistance.

3. Guidelines:

In addressing the above requirements, ISPs should consider these guidelines:

- Offer educational information and resources directly or through referral to third party services.
- Keep educational content concise and focused on the most important things users need to know.
- Ensure that instructions can be followed by an audience of non-technical users.
- Use multiple media, e.g., images, videos, text, captions, etc., and, where helpful, multiple languages to maximize customer understanding and accessibility.
- Help end-users determine if they have a bot infection by providing information or pointing to resources that describe anomalous behaviors of bot infected devices and the availability and use of bot detection software tools or services.

7. Bot Detection

a. Overview

As bots evolve, so must the tools and techniques used for detecting them. The challenge to detection lies in the versatility that bot traffic has achieved to avoid many singular techniques used for detection mechanisms, such as simple pattern matching. Detection may be complicated by the fact that some Internet applications, like distributed host-based caching content delivery networks , online gaming applications, and other such services may exhibit behavior similar to that of malicious bots, and may utilize similar technologies. ISPs should employ care in identifying impacted parties for notification and remediation.

b. Recommended Action:

ISPs can find out about malicious activity and bot compromised end-user devices in a variety of ways:

1. Receiving notifications from external entities, particularly those designed to aid with the overall understanding and real-time dissemination of bot related data. A list of resources is listed in Appendix 2.

2. Deploying capabilities within their networks that aid in identifying potential bot infections.

3. Directing customers to tools, a web portal, or other resources that enable customers to self-identify a potential bot infection.

8. End-User Notification of Potential Bot Infection

a. Overview:

Many end-users are unaware that their devices are infected and operating as bots. As a result, those users and their data remain at risk, and the bots can remain active indefinitely. ISPs should leverage detection efforts described in Section 7 to make customers aware of active infections.

Notifications should be designed to help mitigate bots and the harm they cause. Notifications may include information on what a bot is, means of infection, that bots may have no visible symptoms, and what the notification means. Notifications may also contain or identify other resources such as tools, guides, and services that facilitate infection prevention, verification, and mitigation[*]. They may also provide information on any specific bot(s) detected.

End-user notification may take many different forms. It may be performed directly by the ISP or by third parties on behalf of the ISP. ISPs may directly alert end-users or provide mechanisms that allow end-users to request and receive information on their infection status. Similarly, ISPs might enter into arrangements to enable notifications to be delivered to end-users by other ecosystem participants with whom the end-user has a relationship, such as a provider of an Internet application or service.

The ISP should consider mechanisms that ensure that the customer is easily able to authenticate the notifications as genuine and that such notifications will be difficult to spoof.

Where feasible, the ISP may wish to track receipt of notifications. This may help the ISP better understand the effectiveness of various notification mechanisms.

Each ISP will need to evaluate different notification methods in order to find one best suited for the particular ISP and the particular bot threat. The notification method chosen may need to integrate with existing business processes and existing network

[*] Definition found in Glossary

infrastructure. Research and analysis may be required to develop and maintain appropriate notification systems and policies.

b. Recommended Action:

Provide communication of a suspected bot infection to the customer or help enable customers to determine if they are potentially infected by bots. Many notification methods are outlined in references in Appendix 2; however, other methods may be used.

9. Bot Remediation

a. Overview

Bot mitigation and remediation is the ultimate goal of any bot infection notification program and is ultimately the responsibility of the end-user. Notification alone may be sufficient for technical users but the majority of users usually require some form of assistance in removing bot malware from their infected devices. Remediation, however, can be difficult, and may involve other complex functions such as isolating the source of the infection among many devices sharing an Internet connection; backing up all data and system software ahead of time in a way that preserves the end-users' ability to recover (but doesn't back up the infected files or programs as well); and ensuring that the end-user has source disks and other materials from which to reconstruct their device image if required during the remediation process.

It is understood that some ISPs may not have the resources to provide this level of service, nor be able to support such activities free of charge or even for a fee. In many cases, end-users may need to be referred to providers of professional computer support services to fully remediate their machines. ISP notifications may wish to anticipate this fact and suggest that customers seek third party assistance to avoid frustrating end-users with limited-service help-desks or support lines that aren't capable or equipped to fully address the remediation issues.

b. Recommended Action:

1. Bots are designed to be stealthy and difficult to remove. As part of the notification, ISPs should offer guidance, as described above. This may include links to a variety of publically available online and third party sources of information, software, and tools. It might also include links to professional services. These need not be offered by the ISP itself but may be offered by third parties.

2. An ISP may provide remediation tools to the end-user, either during or after the notification process. However, the ISP should not mandate that the end-user run remediation tools. If the ISP provides tools to the end-user, the end-user should be allowed to exit the process without running any suggested tools or procedures.

3. As part of the notification process, ISPs may wish to include guidance (depending on the nature of the bot in question) that settings on customer owned network equipment such as home gateways and routers may have

been altered and should be restored to a secure state, depending on the nature of the bot infection.

c. Guidelines:

1. Bot removal tools and services must respect user privacy.

2. Possible infection remediation methods are outlined in the CSRIC II WG 8 best practices and in the bot remediation IETF RFC which are referenced in Appendix 2.

10. ISP Collaboration

a. Overview:

Bot mitigation and management are activities in which ISPs, search providers, end-users, IT departments, hosting companies, blog providers, security vendors, researchers, government, financial services companies, cloud service providers, and other parties all have roles. With multi-stakeholder input and collaboration, the results will exceed those possible through independent actions alone. ISPs' participation in this code, along with complementary and collaborative approaches taken by other segments of the Internet ecosystem, can be expected to drive substantial mitigation of the threat posed by botnets.

b. Recommended Action:

Code participation requires collaboration within ISP, industry, or broader fora through collaborative activities, of which the following are examples:

1. Sharing detection, notification, or mitigation methods planned for or deployed in ISP networks, and where practical an evaluation of their effectiveness.

2. Sharing of intelligence or operational attack data that may be useful in bot prevention, defense, or remediation.

3. Identification of key data or technical resources that are needed from systems or actors beyond the ISP network.

4. Participation in definition, development, or operation of integrated defense strategies or systems which extend beyond the boundaries of the ISP network.

5. Other collaboration activities involving the sharing of information with parties outside the ISP or data with systems outside of the ISP network.

All information sharing between ISPs and other involved parties will be performed in accordance with applicable laws including, but not limited to, antitrust and privacy laws.

11. Further Development of this Code

This Code will evolve over time due to the dynamic nature of the bot threat and the experience and assessment of ISPs.

12. Additional Information and Resources

Appendix 1 – Glossary
Appendix 2 – References

Appendix 1 – Glossary:

1. Bot

The following definition draws heavily from “Recommendations for the Remediation of Bots in ISP Networks” (Referenced in Appendix 2):

A malicious (or potentially malicious) "bot" (derived from the word "robot", hereafter simply referred to as a "bot") refers to a program that is installed on a system in order to enable that system to automatically (or semi-automatically) perform a task or set of tasks typically under the command and control of a remote administrator (often referred to as a "bot master" or "bot herder.")

Computer systems and other end-user devices that have been “botted” are also often known as "zombies".

Malicious bots are normally installed surreptitiously, without the user's consent, or without the user's full understanding of what the user's system might do once the bot has been installed.

Bots are often used to send unwanted electronic email ("spam"), to reconnoiter or attack other systems, to eavesdrop upon network traffic, or to host illegal content such as pirated software, child exploitation materials, etc.

Many jurisdictions consider the involuntary infection of end-user hosts to be an example of an unlawful computer intrusion.

2. Botnet

Botnets are networks of Internet-connected end-user computing devices infected with bot malware, which are remotely controlled by third parties for nefarious purposes.
A botnet is under the control of a given "botherder" or "botmaster." A botnet might have just a handful of botted hosts, or millions.

3. Customer (or "Direct Customer")

The party contracting with an ISP for service. Distinguish the "customer" from an "authorized user:" for example, a coffee shop might purchase Internet service from an ISP. The coffee shop would be the ISP's customer. The coffee shop might elect to offer free use of its connection (if permitted by the ISP's Acceptable Use Policy, or AUP) to those who buy coffee from it -- coffee buyers would then be authorized users of the connection purchased by the coffee shop, but not the ISP's direct customer.

4. Detection

Detection is the process whereby a service provider or end-user comes to be aware that a particular system or device has been infected with malicious software. A service provider may detect that a system has become infected many different ways, including as a result of receiving complaints from third parties about spam, network scanning, or attacks that have been sourced from that system. End-users may detect system infections through software tools or other means.

5. Ecosystem

This term is often used to describe the interrelationship of various Internet participants—the hardware manufacturers, software developers, ISPs, and providers of various Internet content, applications, and services that make the Internet work and be useful for end-users.

The internet ecosystem includes operating system vendors, end-user focused organizations, providers of Internet content, applications, and services, ISPs, search providers, end-users, IT departments, hosting companies, blog providers, security vendors, researchers, government, financial services companies, and other parties.

The so-called "underground economy" is also often described as an "ecosystem," with multiple participants filling diverse specialized roles. For example, some participants may specialize in writing malware, while others may "harvest" email addresses from web pages and mailing lists, while still others may specialize in distributing malware to those harvested email addresses. The malware ecosystem will also normally include the population of targeted potential victims, and law enforcement agencies working to combat cybercrime.

6. End-user

End-User: In a computing and networking context, the end-user is the person who ultimately makes authorized use of a product or service.

The end-user may often not be the same as the person who may have purchased the product or service. For example, a coffee shop owner may purchase connectivity for use by his or her customers; in that scenario, the coffee shop customers, and not the coffee shop owner, represent the actual "end-users," even though they did not directly contract with an ISP for the connectivity they're using.

A party, such as a hacker/cracker who makes use of a product or service without the authorization of the purchaser, would normally be considered a cyber intruder and not an "end-user" per se.

7. ISP

An Internet Service Provider (ISP) is a company that provides retail access to the Internet for members of the public, or for businesses and other organizations. Those connections may be via cable, DSL, satellite, wireless, dialup, or other technologies. ISPs are sometimes also known as "access providers."

An enterprise that provides access to the Internet solely for its own employees would not normally be considered to be an ISP. Likewise, a network carrier that only provides wholesale access to the Internet for other ISPs would normally be considered to be a network service provider (NSP), rather than an ISP.

8. Malware

"Malware" is short for "malicious software."

Malicious bots are one type of malware. Other forms of malware include categories of software known as viruses, Trojan horses, worms, rootkits, crimeware, keystroke loggers, dialers, spyware, adware, etc. The factors that distinguish those different types of malware are less important than an understanding of why malware may be viewed as "malicious."

Malware often violates one or more of the following fundamental principles:

(a) Consent: Malware may be installed even though the user did not knowingly ask for that to happen.

(b) Honesty: Malware may pretend to do one thing, while actually doing something completely different.

(c) Privacy-Respectfulness: Malware may violate a user's privacy, perhaps capturing user passwords or credit card information.

(d) Non-Intrusiveness: Malware may annoy users by popping up advertisements, changing web browser's home page, making systems slow or unstable and prone to crash, or interfering with already installed-security software.

(e) Harmlessness: Malware may be software that hurts users (such as software that damages our system, sends spam emails, or disables security software).

(f) Respect for User Management: If the user attempts to remove the software, it may reinstall itself or otherwise override user preferences.

It all adds up to "software users just don't want."

Users may unknowingly install malware by opening a tainted attachment received by email, or by visiting a web page that has malicious content. Systems may also be directly infected by a remote attacker as a result of the attackers targeting a known vulnerability that may be remotely exploitable, or by the user mounting an infected CD, DVD, or thumb drive.

9. Mitigation

Mitigation is the process of managing or controlling the effects associated with a bot. For example, if a system is infected with a spam bot, and is spewing unwanted commercial email, mitigation may consist of filtering the spam that is being emitted from that device.

Note that mitigation typically does not involve fixing the underlying condition (that would be "remediation"); mitigation just manages the symptoms associated with a condition.

10. Notification

Notification is a process whereby ISPs communicate with their end-users regarding the possible infection of the end-user’s device by bot malware or how a subscriber can prevent or identify such an infection. Notification may also entail a process whereby end-users are directed to tools that will enable self-discovery of bot infections. Notification can take different forms, including direct notification by the ISP to the end-user, or indirect notification through available self-discovery tools or a third party. Notification may be done via multiple potential channels, including (but not limited to) e-mail, postal mail, a phone call, in-browser notification, web-based self-discovery tool, or SMS message.

11. Prevention

Prevention is the process of hardening a system or service so that it is less vulnerable to compromise and exploitation. For example, on many systems, prevention may involve:

— Patching the operating system and all applications with available security fixes
— Installing or enabling a firewall
— Using anti-virus software
— Making sure the system is regularly backed up
— Using strong passwords
— Disabling all unneeded network services
— Encouraging users to safely use internet services (e.g., e-mail, web browsing, etc.)

12. Remediation

Remediation is the process that an end-user goes through to clean up a botted computer so that it is no longer infected. In easy cases this may involve installing and running an anti-virus product. In more difficult cases, remediation may involve more substantial intervention up to "nuking and paving" the system -- formatting it and reinstalling it from scratch, or at least from the last known-clean backup. Once the system is clean, or has been reinstalled, it will then normally be hardened to protect it from reinfection.

13. Spam

Unwanted and unrequested e-mail, often commercial in nature, normally sent to a large number of recipients in substantially identical form. Spam is often sent by "affiliates" who are paid by the person running the affiliate program when recipients purchase the spamvertised product.

Appendix 2 – References

1. Recommendations on how to manage the effects of computers infected with malicious bots: “Recommendations for the Remediation of Bots in ISP Networks”

http://tools.ietf.org/rfc/rfc6561.txt

2. CSRIC II Working Group 8 - ISP Network Protection Best Practices

http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf

3. icode – Australian Internet Industry Code of Practice addressing cyber security

http://iia.net.au/images/resources/pdf/icode-v1.pdf

4. Japan Cyber Clean Center – Anti-Botnet Project

https://www.ccc.go.jp/en_index.html

5. German Anti-Botnet Advisory Centre – Anti-Botnet Project

https://www.botfrei.de/en/

6. Japan Computer Emergency Response Team (CERT)

http://www.jpcert.or.jp/english/

7. US CERT - Understanding Hidden Threats: Rootkits and Botnets

http://www.us-cert.gov/cas/tips/ST06-001.html

8. Alliance for Telecommunications Industry Solutions (ATIS)

http://www.atis.org/

9. Department of Homeland Security

http://www.dhs.gov/files/programs/gc_1158611596104.shtm

10. Department of Homeland Security - United States Computer Emergency Readiness Team (US-CERT)

http://www.us-cert.gov/

11. International Telecommunication Union Botnet Mitigation Toolkit

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

12. U.S. Commerce Department's National Institute of Standards and Technology (NIST)

http://www.nist.gov/index.html

13. Department of Commerce/Department of Homeland Security Request for Information - Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware

http://www.gpo.gov/fdsys/pkg/FR-2011-09-21/pdf/2011-24180.pdf

14. Comments Received in Response to Department of Commerce/Department of Homeland Security Request for Information - Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware

http://www.nist.gov/itl/botnetcomments.cfm

15. Messaging Anti-Abuse Working Group (MAAWG.org) - Code of Conduct

http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf

16. M3AAWG Collection of Best Practices for ISPs and Network Operators

http://www.maawg.org/published-documents

17. National Vulnerability Database – National Institute of Standards and Technology

http://nvd.nist.gov/

18. Internet Storm Center

http://isc.sans.edu/index.html

19. Shadowserver Foundation

http://shadowserver.org

20. Spamhaus Policy Block List

http://www.spamhaus.org/pbl/

21. Composite Blocking List

http://cbl.abuseat.org

22. OnGuard Online

http://www.onguardonline.gov/default.aspx

23. IETF BCP38 Network Ingress Filtering

http://tools.ietf.org/html/bcp38