Software & Information
Industry Association
1090 Vermont Ave NW Sixth Floor
Washington, DC 20005-4095

November 14, 2011

U.S. Department Of Commerce
U.S. Department Of Homeland Security
[Docket No. 110829543–1541–01]
Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware

The Software & Information Industry Association (SIIA) thanks the Departments of Commerce and Homeland Security for leading this effort to craft a framework to address the problems raised by botnets and related malware.[1] We appreciate this opportunity to provide comments on their proposed framework.

We endorse the fundamental idea of a voluntary approach in which the government convenes the relevant various parties for discussions on best practices. In particular, we support multi-stakeholder discussions on how the private sector can develop and maintain timely and voluntary programs to detect and notify end-users that their machines have been infected with botnets or other malware and provide mitigation support that will eliminate these infections. We ask for the opportunity to be part of these ongoing discussions.

SIIA is the principal trade association of the software and digital information industry, with more than 500 members that develop and market software and electronic content for business, education, consumers and the Internet. As leaders in the global market for software and information products and services, many SIIA members provide products and services that protect businesses, consumers and the public sector from cyber-attacks, viruses, and a wide range of online security threats.

The problems created by malicious software that can turn computers into elements in a robot network (botnet) are well known. These infected computers can be activated by outside entities to launch denial of service attacks, send spam, or harvest personal information such as credit card numbers that can be used for fraud, identity theft or terrorist financing. These problems harm those whose computers are infected when fraudsters copy confidential files, steal online banking credentials, or fraudulently redirect traffic for financial gain. But they also inflict harm on other parties including the computer networks themselves and other sites that might be victims of denial of service attacks.[2]

[1] See the Notice at http://www.federalregister.gov/articles/2011/09/21/2011-24180/models-to-advance-voluntary-corporate-notification-to-consumers-regarding-the-illicit-use-of#p-4

[2] For further discussion of the general problem of botnets, see Tyler Moore, Richard Clayton, and Ross Anderson Economics of on line Crime, Journal of Economic Perspectives, Volume 23, Number 3, Summer 2009, Pages 3–20 available at http://people.seas.harvard.edu/~tmoore/jep09.pdf. See also Symantec,

Tel: +1.202.289.7442
Fax: +1.202.289.7097
www.siia.net

The extent of the problem is hard to quantify exactly, but in the aggregate it undoubtedly imposes substantial economic costs on individuals and enterprises. McAfee estimates that 4 million new computers are infected every month.[3] Individual botnets themselves are enormous. According to McAfee, Bredolab infected 30 million computers, Mariposa 12 million and Conficker 10.5 million.[4] Three quarters of all Internet traffic is spam,[5] and 80% of spam comes from infected computers.[6]

The problem is international in scope, with botnets originating in one part of the world infecting computers globally. In 2010, the United States had the most bot-infected computers, accounting for 14 percent of the worldwide total. Meanwhile, the United States was also the location for the most bot command-and-control servers, with 37 percent of the total. The United States was the top country of attack origin in 2010, accounting for 24 percent of worldwide activity (although only second to Brazil in terms of bot-generated spam traffic, with, respectively, 10% and 8% of the total). The United States is also the world's largest victim of problems associated with botnets. In 2010, it was the country most frequently targeted by denial-of-service attacks, accounting for 65 percent of the worldwide total.[7]

Given the extent of the problem, the strain it puts on public computer networks and the risks it poses both to those whose computers are infected and to the victims of botnet attacks, the need for action is clear. But are the private incentives for fixing the problem strong enough to call forth the resources needed to prevent infection and to mitigate the harm once infection has occurred? Some doubt that private sector incentives are large enough.[8] Self-help by users can go part of the way toward addressing the problem.[9] But these measures are not sufficient. The problem is that financial incentives are not completely aligned. The losses associated with botnets are widely distributed and no single entity in the system of end users, network companies and victims has both the incentive and the means to fix the problem on its own.

Collaboration and cooperation are needed to address the problem in a holistic way. Some suggest a government role to subsidize the notification and mitigation efforts needed to clean up infected

---

http://us.norton.com/theme.jsp?themeid=botnet and McAfee, Botnets Demystified and Simplified http://blogs.mcafee.com/mcafee-labs/botnets-demystified-and-simplified

[3] McAfee Quarterly Threat Report 2nd Quarter 2011: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q2-2011.pdf

[4] McAfee, Botnets Demystified and Simplified at http://blogs.mcafee.com/mcafee-labs/botnets-demystified-and-simplified

[5] Symantec Intelligence Report, October 2011, p. 7 http://www.symanteccloud.com/globalthreats

[6] McAfee, Botnets Demystified and Simplified at http://blogs.mcafee.com/mcafee-labs/botnets-demystified-and-simplified

[7] Symantec, Global Internet Security Threat Report, Vol. 16, April 2011. http://www.symantec.com/business/threatreport/

[8] van Eeten, M. J. and J. M. Bauer (2008), "Economics of Malware: Security Decisions, Incentives and Externalities", *OECD Science, Technology and Industry Working Papers*, No. 2008/01, OECD Publishing. doi: 10.1787/241440230621

[9] See for example the best practices and guidelines for users and enterprises offered by Symantec in their Intelligence Report, October 2011, p.16 http://www.symanteccloud.com/globalthreats

computers.[10] In this model, researchers inform network companies (or they become aware through their own traffic monitoring activity) of IP addresses of infected computers on their networks. The network companies communicate with the customer whose computer appears to be infected and offer them a government-sponsored clean-up scheme, which they are entitled to use if they wish.

There are initiatives in other countries to provide a collaborative framework that follow this rough model. In Australia, the Internet Industry Association developed a code of best practices for the industry. In this system, a government agency, the Australian Communications and Media Authority (ACMA), collects information on IP addresses of infected computers and distributes that information to the Internet service providers. The ISPs then provide this information to their customers and provide advice on how to fix it. Participation in the initiative is voluntary, but ISPs accounting for 90% of Australian Internet users have joined. The cost of monitoring for infected computers is not borne by the ISP, but they are responsible for the cost of removing the malware from their customers' computers.[11]

Japan's Cyber Clean Center also provides an example of a collaborative effort to address the problem. It is organized by the Japanese Computer Emergency Response Team Co-ordination Center (JPCERT). ISPs representing 90% of Japan's Internet users have joined. ISPs receive information on infected computers and communicate with their users, directing them to a website that allows them to download a clean-up tool. Neither the monitoring nor the clean-up costs of the program are born by the ISPs.[12]

In the United States, Comcast has developed a voluntary program called Comcast Constant Guard, under which the company will provide information to its users when a computer may be infected with a bot. The company then refers them to the Comcast Constant Guard Center for important information on how to remove the malicious software. Under an arrangement with McAfee, Comcast provides a clean- up service for a fee.[13]

Search engines are also taking steps to warn users that their computers might be infected. In July 2011, Google discovered that some unusual traffic connecting to its search engine was caused by computers infected with a specific strain of malware. Google responded by displaying a

---

[10] Richard Clayton, "Might Governments Clean up Malware?" Workshop on the Economics of Information Security, June 2010 at http://weis2010.econinfosec.org/papers/session4/weis2010_clayton.pdf

[11] A description of the program can be found here: http://icode.net.au/. See also OECD (2011), "ISPs and malicious software (malware) security threats", in OECD, The Role of Internet Intermediaries in Advancing Public Policy Objectives, p. 114, OECD Publishing. doi:10.1787/9789264115644-9-en

[12] The Japanese Cyber Clean Program is described here: https://www.ccc.go.jp/en_ccc/. See also OECD (2011), "ISPs and malicious software (malware) security threats", in OECD, The Role of Internet Intermediaries in Advancing Public Policy Objectives, p. 112, OECD Publishing. doi:10.1787/9789264115644-9-en

[13] Comcast's program is described here: http://security.comcast.net/constantguard/

prominent warning at the top of its search results page when it appeared that a user's computer was infected with this malware.[14]

Some voluntary best practices have been proposed. The Computer Security, Reliability and Interoperability council (CSRIC) has issued best practices for ISPs to consider in responding to bot net problems.[15] The Internet Engineering Task Force also has developed a draft "Recommendation for the Remediation of Bots in ISP Networks.[16]

Despite these efforts, SIIA believes that there would be great benefit from further discussion of collaborative efforts to address this problem. We have several points to further this discussion.

- A voluntary code of conduct approach is preferable to regulatory intervention.
- ISPs need to be involved because they have a privileged role in the infrastructure.
- Other participants should include security firms, search engines and computer services companies.
- Awareness of the problem needs to be increased across all sectors.
- Prevention should be promoted to the consumer.
- Detection of the problem can involve technology vendors who can step in either in support of or together with ISPs.
- Notification should remain in the remit of ISPs, making sure that the process of notification itself is secured against maliciously exploitation.
- Offering free-of-charge cleaning tools and consumer support facilities has shown benefit, but consumers would also benefit from value-added services.
- Foreign experience suggests that the best model is private operational management with public support.
- Information sharing is crucial, but companies need liability protections for notifying consumers that their devices have been infected by botnets.

The Notice suggests that "voluntary codes of conduct developed through a multi-stakeholder process can significantly advance efforts to protect the Internet from the growing security threats." One of its policy recommendations is "for Commerce to expand its role of working with multiple stakeholders to facilitate and promote the use of voluntary codes of conduct." The Notice concludes that "this facilitating role in the area of codes of conduct is seen as vital to advancing industry efforts in specific areas."

---

[14] The Google program is described here: http://www.google.com/support/websearch/bin/answer.py?answer=1182191. See also David, Goldman, "Google notifies users of malware infections," CNNMoney, July 21, 2011 at http://money.cnn.com/2011/07/20/technology/google_malware/

[15] See Internet Service Provider (ISP) Network Protection Practices December 2010 at Http://Transition.Fcc.Gov/Pshs/Docs/Csric/Csric_Wg8_Final_Report_Isp_Network_Protection_20101213.Pdf.

[16] Available at http://tools.ietf.org/id/draft-oreirdan-mody-bot-remediation-03.html.

SIIA welcomes this facilitation role in the case of collaborative efforts to manage the botnet problem. We urge that the agencies act as the convener and facilitator providing a platform for the airing and discussion of the views of industry, non-governmental organizations, technical experts and international participants. We also want to make sure that the codes that emerge from this process are voluntary self-regulatory standards, not de facto regulatory mandates.

We urge the Department of Commerce and Homeland Security to move ahead with such an effort, and ask that SIIA be part of these on-going discussions. If you have any questions, please do not hesitate to contact me or Mark MacCarthy, Vice President for Public Policy at (202)289-7442 or mmaccarthy@siia.net.

Sincerely yours,

Ken Wasch
President