Comments on FCC cybersecurity roadmap RFC (Docket No. 10-146)
Maxim Weinstein on behalf of StopBadware, Inc.
September 23, 2010

Overview

StopBadware is a 501(c)3 non-profit organization that works with corporate partners—Google, PayPal, and Mozilla—and a broad community to fight malware. We started our existence as a project of the Berkman Center for Internet & Society at Harvard University before spinning off earlier this year. StopBadware's knowledge of malware trends, and our particular experience with the distribution of malware through the web, may provide valuable lessons and parallels relevant to the FCC's interest in securing communications networks and their users.

Malware has for several years been a persistent and growing threat to end users, be they individual consumers or business users. It is difficult to find reliable data about the total impact of malware, but Consumer Reports estimates $3.9b in damage to U.S. households alone from viruses and spyware over the past two years.[1] (That figure does not include financial losses due to spam, phishing, and other threats that are supported by the malware ecosystem.) Malware can turn a computing device into a *bot* or *zombie* which is networked with other infected devices into *botnets*, posing a particular threat to communications networks. The operator of a single botnet can harness the collective power of thousands of PCs simultaneously to attack specific targets or to spread additional malware and spam.

Earlier this year, StopBadware—in collaboration with the National Cyber Security Alliance (NCSA) and the Anti-Spyware Coalition—commissioned a report to identify the many parties influencing the spread of malware via the web. This report (attached), "A Broader Look at Web-Based Malware: Mapping the Threat to Better Fight It," presents a model, known as the Chain of Trust, for illustrating the actors and relationships that affect particular interactions online. The specific chain related to web malware, shown on page 27 of the report, helps illustrate the roles of several categories of communications providers: consumer ISPs, upstream/backbone providers, web hosting providers, and web hosting resellers. Probably most relevant to this FCC inquiry is the role of the consumer ISP, which will be explored further below. It might also be worth considering whether the Chain of Trust model could be applied to other security-sensitive interactions involving users and communications providers of interest to the Commission.

The role of broadband ISPs

As indicated by the Chain of Trust diagram, broadband Internet Service Providers (ISPs) interact directly with users as trusted vendors. This gives them several opportunities to affect the malware landscape, especially botnets formed by the presence of malware on customers' computing devices. Notes on

---

[1] http://www.consumerreports.org/cro/magazine-archive/2010/june/electronics-computers/social-insecurity/state-of-the-net-2010/index.htm

several areas where ISPs could—and in some cases already do—have an impact, along with notes on a potential regulatory role and parallels to StopBadware's work with websites, follow.

Detection of malware/bot behavior

Because they carry all Internet traffic to and from their customers, ISPs are in a unique position to detect bots and other forms of malware that spread or communicate across the network. There are many mechanisms for detection, covering a wide range of accuracy and invasiveness. It will be critical to ensure that ISPs strike the proper balance between using their power to protect the network and abusing that power in a way that compromises user privacy.

In the current market, there may be a lack of incentives for ISPs to implement detection programs (such a program may be costly and may not correlate to increased revenues/profits for the ISP). ISPs may also fear the consequences of having the information: subpoenas requesting the data, potential liability if they knew but didn't act on knowledge of a bot, pressure to share the data (see next section). ISPs may also not have the knowledge or resources necessary to implement a high quality bot detection program. Such a program requires systems that can analyze network traffic in large volumes without affecting network performance. Several vendors offer such systems, but they tend to be expensive and complex. A major concern for consumers involves privacy, as some malware detection techniques use deep packet inspection or other techniques that can also be used for monitoring customers' Internet traffic or tracking their online behavior.[2]

These concerns raise several opportunities for intervention by industry groups, the Commission, Congress, and/or third-party organizations:

- Increase the incentives for ISPs to actively detect malware behavior using non-invasive approaches. One possible incentive would be a "Good Housekeeping" seal that indicates an ISP's efforts to prevent and detect malware. Of course, with many households in the U.S. having limited choice of broadband provider, it's unclear whether this would provide a suitable competitive advantage to become an incentive. If industry is unable or unwilling to meet its responsibilities to both security and privacy through self-regulation, and if other economic levers (including those below) are insufficient to induce change, it may be appropriate to consider regulation.
- Limit liability. There may be certain expectations (see sections below) about what an ISP should do once it is aware of malware activity. Limiting the ISP's liability if it complies with those expectations might encourage ISPs to voluntarily detect malware.
- Provide resources. A centralized organization could provide resources—data, guidance, financial support, and/or technology—to ISPs to help support them in implementing malware detection systems.

---

[2] See, for example, the recent controversy over UK ISP TalkTalk's implementation of a malware detection program.

- Create privacy and disclosure guidelines. A clear set of guidelines—based on a detailed understanding of the security needs, the available technology, and the privacy concerns involved in malware detection—would provide a common measuring stick for ISPs. This could be a regulatory function, though it's also possible that a third-party organization could develop guidelines and provide monitoring and reporting on ISPs' compliance.[3]

Reporting of detected malware/bots

If an ISP implements a detection program, the data is clearly useful to the ISP itself, and to the ISP's customers (see next section). Less obvious is the value of the data to a variety of other organizations. Law enforcement, for example, can use the data to investigate crimes or attribute specific malware to particular criminal groups. Security research organizations, like ShadowServer and Team Cymru, use aggregated bot data to report on trends, find so-called "command and control" servers, and disrupt botnets. Government and non-profit monitoring organizations may use data to measure the total impact of malware or to track ISPs' effectiveness in controlling malware on their networks.

In StopBadware's experience working with similar data (detections of badware websites), it is often challenging to get companies to share data freely. A web hosting provider, for example, may be reluctant to acknowledge the number of its customers' sites that have been infected, the types of infection, the mechanisms for infection (which, in some cases, might reveal proprietary business information about how systems are configured/managed), or the total number of sites the company manages (which is helpful to evaluating the *rate* of infection).

ISPs may be less reluctant than hosting providers, as an infected customer PC does not implicate the ISP as much as an infected website implicates the company that operates the web server. Furthermore, many law enforcement and security organizations are willing to maintain privacy of data, which can allay some ISPs' concerns. Getting ISPs to voluntarily share data for public reporting of infection and remediation rates, however, might be a challenge that require regulatory intervention.

Customer notification

Whether an ISP detects malware on its own or learns of infected customer devices through a third party, the ISP is in a unique role to identify the specific household in which the device is operating. This implies a responsibility on the part of ISPs to notify their customers. Again, however, the incentives may not be aligned. Notifying customers takes time and money. Once notified, customers are likely to turn to the ISP for support in finding and removing the malware, which can be very costly and time consuming, as well as being outside the scope of an ISP's core business. Notifications also create their own challenges, as they might be imitated to trick users into buying fake anti-virus software or otherwise giving up

---

[3] Early in its life, StopBadware worked with industry partners, academics, security experts, and the community to develop "badware guidelines" for software applications. SBW then reported on products that failed to meet these guidelines. This was effective in moving companies that sought market legitimacy to move away from "sneaky" application behavior and towards better disclosure and user control.

money (or personal information) to a rogue actor. A draft IETF document[4] written by Michael O'Reirdan, et. al., of Comcast addresses some of the options—and obstacles—to customer notification.

Globally, several ISP customer notification efforts are underway. One of the most sophisticated—and one that the Commission should examine in detail—is the Australian Internet Security Initiative (AISI).[5] The AISI is a government-led effort to collect bot data from multiple providers, parse it out by specific ISP, and feed the data to the relevant ISPs. Those ISPs agree, in exchange for the data, to notify their customers about the infected machines. This process ties into the Australian Internet Industry Association's icode[6], which is a voluntary code of conduct for ISPs that includes education, detection, action, and reporting related to customer bots. ISPs that adhere to the code can display a participation logo, and the participation rate is reportedly high.

Germany has instituted a national effort similar to that of Australia. Individual ISP efforts, including those of Comcast in the U.S. and Virgin Media in the U.K. are worth exploring, as well.

Quarantining of infected customers and blocking of malware traffic

More controversial roles for ISPs include quarantining infected customers and blocking malware traffic. The former involves disconnecting the customer from the Internet completely or, more commonly, placing the customer into a "walled garden" that allows access only to an ISP-determined set of sites that can help the customer remove the malware. Malware blocking uses known signatures, addresses of known botnet command & control servers, and/or suspicious traffic patterns to prevent a customer's device from communicating with remote systems. The intent of both these approaches is to prevent the further spread or impact of the malware. The quarantine approach also creates an incentive for the customer to address the root problem by removing the malware.

One concern with both of these approaches is the substantial negative impact on the customer if the system has a false positive (i.e., detecting malware when none is present) or if the quarantine/block doesn't end quickly once the malware is removed. StopBadware has some experience with this concern, as we work with partners (Google and Mozilla) that warn users to avoid known badware websites. Both the visitors and owners of these sites face a negative consequence if a website is listed as badware inaccurately or longer than necessary. To help combat this, StopBadware offers an independent review process that helps website owners ensure that their sites are removed from badware lists in the case of false positives or after a site has been "cleaned."[7] Having such independent oversight, along with a responsive and understandable process for addressing these concerns, will be critical for any ISP planning to implement quarantining or blocking.

 In the case of walled gardens, an additional concern is the potential for anti-competitive or other negative consequences that result from the ISP being a gatekeeper. For example, the ISP could offer a fee-based service for remediating malware, and block the customer from accessing or researching other

---

[4] http://tools.ietf.org/html/draft-oreirdan-mody-bot-remediation-09
[5] http://www.acma.gov.au/WEB/STANDARD/pc=PC_310317
[6] http://iia.net.au/images/resources/pdf/icode-v1.pdf
[7] Google also offers its own automated systems for removing "cleaned" sites quickly from its badware list.

such services. Similarly, the ISP could offer access to the website of a single anti-virus provider (perhaps one that has a financial relationship with the ISP), and block access to the many other anti-virus products (including free products) available in the market. One possible approach that could be encouraged or required by the Commission, is to require walled gardens to provide access to a government or non-profit website with objective information (and perhaps tools) to help customers find and remove malware. This is the approach currently being tested in Germany.

All forms of quarantining and blocking should recognize the need for security researchers to conduct research into malware. This might, for example, require a researcher who is a customer of an ISP to access servers known to be malicious. A researcher might also want to allow a bot to continue operating—in cooperation with the ISP—so that the bot's traffic and behavior can be analyzed. ISPs should be expected to comply with reasonable requests from customers and external researchers that have a valid reason to take actions that might otherwise be blocked on the network.

Remediation

When a customer's computer is infected with malware, the customer may turn to the ISP for help in removing the malware, especially if the ISP notified the customer of the problem in the first place. This creates a challenge for the ISP, which as previously noted may not have the resources or expertise to assist the customer. Exacerbating this challenge is that removing malware is often complex: it is dependent on the user's system and configuration, and there is no one-size-fits-all solution. Sometimes, even identifying the affected *device* can be a problem. A single household's home network might include two or three PCs, a network printer, a router, a digital video recorder, and other Internet-connected devices. From the standpoint of many bot-detection systems, the malware will originate from the IP address of the customer, but it may not be obvious which device(s) is/are infected. (In most cases, the particular type of malware will give a hint as to whether the device is a Windows computer, a router, a printer, etc., but identifying the specific computer can be a challenge.)

Some ISPs have experimented with offering malware remediation as a fee-based service, but this raises concerns—both real and perceived—about a conflict of interest, especially if the ISP is detecting and notifying customers about the malware. Other ISPs, such as Comcast, have offered a limited set of free tools to help with detection and removal, but have not completely figured out how to help those for whom the tools are insufficient.

Again, StopBadware has some experience here, as we work with website owners whose sites have become infected with badware. In addition to educational content on our website, we offer an online community[8] that allows site owners to request assistance from volunteers. This supplements or substitutes for each of our partners and data providers operating their own remediation programs. It also establishes StopBadware and our online community as a nexus of expertise in this area. This, in turn, encourages the exchange of knowledge amongst members of the community, which further strengthens our ability to prevent and remediate badware website infections. The centralized community has also helped support the development of a market for value-added remediation and prevention services. A

---

[8] http://www.badwarebusters.org

similar approach, with an independent organization offering "one-stop shopping" for remediation of bots and other end user device malware, could be effective in addressing this issue for ISPs. Such an organization could be funded by government, industry, and/or individual donations.

Preventive education and tools

Because of their relationships with customers, ISPs are in a position to provide educational content and tools to help their customers keep malware off their personal devices. Several domestic and international ISPs offer security portals (with links and content about how to stay safe online), and many leverage partnerships with anti-virus vendors to offer free or reduced cost software to their customers.

At StopBadware, we have not researched the effectiveness of these programs in detail. Based on anecdotal evidence, however, we believe they may have limited value, for a few reasons:

- We have heard that adoption rates of ISP-provided anti-virus software are low. This is likely due to the large number of other avenues by which users acquire AV software: free products from companies like Microsoft, AVG, and Avast; free trials of AV software bundled on new PCs; pre-installed AV software sold as add-ons by retailers; etc.
- Security portals and other preventive education content is often less prominent to users than ISP marketing materials or sponsored content. Much of it is "pull" rather than "push" content, meaning that users have to choose to go look for it, rather than having it delivered in ways they can't miss.
- Generally, users are inundated by messaging about security from many directions: media, security vendors, PC vendors, retailers, ISPs, educators, etc. Often the messaging is confusing and contradictory. In addition, much of it is not actionable (it describes a threat or provides vague instructions, without offering specific guidance on what the user should do).

Some of these issues could be addressed by coordinating messaging across ISPs and other industry players. This could come in the form of a single shared site, similar to StopBadware's centralization of badware website remediation resources. It could also be a common set of content developed independently but then presented by ISPs through their choice of delivery mechanisms. Finally, it could be ISP-specific content that follows a common messaging framework, such as that being developed by the NCSA and the Anti-Phishing Working Group. In each case, a focus on short, clear, actionable messaging, easily seen by the customer, would increase the value to the customer and ultimately the security of the network.

Summary/conclusion

Malware is a major threat to communications networks and their users, and broadband ISPs have the opportunity to do more than they are now to mitigate this threat. It is our hope that this independent look at some of the challenges and potential solutions will help the Commission set priorities and take appropriate action. If anyone from the Commission would like to speak with us for additional input, please contact us using the information below.

Respectfully,
Maxim Weinstein
Executive Director

StopBadware
PO Box 380295
Cambridge, MA 02238