Before the

Department of Commerce
National Institute of Standards and Technology
National Telecommunications and Information Administration

Department of Homeland Security

Washington, D.C.

In the Matter of	)	
	)	
Models to Advance Voluntary Corporate	)	
Notification to Consumers Regarding the	)	Docket No. 110829543–1541–01
Illicit Use of Computer Equipment by	)	
Botnets and Related Malware	)	
	)	

COMMENTS OF VERIZON AND VERIZON WIRELESS

As providers of communications services to millions of customers around the world, Verizon and Verizon Wireless (collectively "Verizon") address cyber attacks daily and have developed a wide range of measures intended to help protect their networks and the networks of their customers. Verizon shares the concerns expressed in the *Request*[1] regarding the threat presented by botnets, which reportedly have established a persistent and growing presence among Internet-connected systems. Verizon applauds the Department of Commerce and Department of Homeland Security for recognizing that the most effective way to combat botnets is through "voluntary" efforts "developed through a multi-stakeholder process."[2]

---

[1] *Models To Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware*, Request for Information, Docket No. 110829543–1541–01, 76 FR 58466 (2011) ("*Request*").

[2] *Id*. at 58467.

As the Departments and other sectors of the government move forward to address *any* cybersercurity issue – not just botnets – they should ensure that their efforts are coordinated and include all entities involved in the Internet ecosystem. Limiting the conversation to only ISPs would not only unfairly impose burdens on one segment of the Internet ecosystem, but also lead to a less effective response to a cyber threat. Moreover, the government should espouse the voluntary approach in the *Request* as it moves forward on cybersecurity to preserve private entities' flexibility to adopt appropriate, timely responses and develop innovative solutions to cyber threats.

Finally, the government should focus its efforts at enhancing cybersecurity in areas where it is best situated to provide assistance. In particular, the government should develop more effective programs to educate consumers on cybersecurity risks and best practices, remove legal and non-legal barriers to information sharing, and step up its law enforcement activity and international coordination efforts.

DISCUSSION

I. The Government Should Ensure That Its Cybersecurity Efforts Are Coordinated and Inclusive.

Coordination and inclusiveness are important in order to most efficiently address the threat of cyber attacks. Not only should all government entities work together to support a unified approach to cybersecurity, but that approach must embrace all participants in the Internet ecosystem. Cybersecurity is not just an issue for ISPs.

A. The Government Should Coordinate Its Various Cybersecurity Efforts.

Given the wide-spread level of concern across all government sectors on cybersecurity issues, it is not surprising that many different proposals exist for how to

best address these issues. However, duplicative or inconsistent initiatives threaten to drain scarce resources and divert industry from substantive cybersecurity activity.

For example, over the past few years, Senators Rockefeller and Lieberman have each introduced comprehensive cybersecurity legislation – which have been passed out of their committees (Commerce, Science, and Transportation and Homeland Security and Government Affairs, respectively) – that would establish a formal government role and place certain requirements on providers of critical infrastructure. The Senate has been reportedly working to merge the various draft bills.

In addition to the legislative branch, the Department of Homeland Security and the National Security Agency have long been responsible for developing defenses to cyber attacks. And last year, the Federal Communications Commission (FCC) issued a Notice of Inquiry regarding a voluntary cybersecurity certification program and a public notice for a cybersecurity roadmap.[3]

Indeed, as the Departments are aware, the FCC is currently examining the topic raised in the *Request* – i.e., establishing a voluntary code of conduct with respect to the botnet issue. The FCC's Communications Security, Reliability, and Interoperability Council (CSRIC), which is comprised of FCC staff, ISPs, and other industry participants, has been focused on botnet detection, notification, and mitigation for well over a year. A CSRIC Working Group (WG 7) is currently exploring this issue.

These various ongoing efforts could result in inconsistent, duplicative, or wasteful recommendations on botnets. The government should ensure that all government entities

---

[3] *See Cyber Security Certification Program*, Notice of Inquiry, 25 FCC Rcd 4345 (2010); *FCC Seeks Public Comment on National Broadband Plan Recommendation to Create a Cybersecurity Roadmap*, Public Notice, 25 FCC Rcd 10570 (2010).

have a unified approach on cybersecurity to avoid substantial inefficiencies and potential conflicts among competing initiatives.

B. Coordination Across Entities in the Internet Ecosystem Is Required.

Government efforts to improve cybersecurity must also be inclusive, embracing all members of the Internet ecosystem. In the botnet context, the *Request* appropriately acknowledges that "security flaws in the hardware and/or software used by individual consumers" are a primary contributor to the botnet problem.[4] Yet many discussions of the botnet issue tend to focus solely on actions that ISPs should take, as though ISPs were the only part of the ecosystem with a role to play.

Any solution to a cyber threat, such as botnets, requires the participation of the full industry. For example, hardware vendors and in particular software manufacturers and developers, including operating systems providers, have important roles as their products may have weaknesses that cyber criminals seek to exploit. Software updates and patches may prove to be key defensive tools to cyber attacks if vendors develop, test, and deploy patches on a regular basis and end-users are encouraged and able to adopt such patches. On the other hand, ISPs cannot develop such updates or patches and have no unique ability to distribute them to end users and assist in their implementation.

In addition, a wide range of Internet content, application, and service providers may be able to assist in addressing the botnet issue. As noted below, notification to infected end users might reasonably be accomplished by a number of means. In that same vein, non-ISP providers of Internet services, such as domain name service, may be able to assist in various ways. And because end users have established relationships with

---

[4] *Request* at 58467.

a wide range of Internet ecosystem participants, those participants may be the best source for end user education and botnet notification in many cases.

Entities other than ISPs are likely to have unique perspectives, expertise, and end user relationships that might prove quite useful in collective efforts to combat cyber threats. Their engagement may lead to the development of solutions that are far more effective and less costly than if ISPs acted alone.

II. The Government Should Promote an Environment That Maximizes ISPs' Flexibility and Preserves Speed of Response.

Notwithstanding the need for broad engagement on cybersecurity issues, ISPs do have a role to play, and ISPs are embracing that role. In that regard, network providers must retain the freedom to implement any measures to secure their infrastructure and critical systems, including the freedom to take rapid, decisive action without being subject to regulatory second-guessing. ISPs also require the latitude to experiment with various technical and business-model solutions to best address the wide range of issues involved in cybersecurity.

A. Any Government-Sponsored Best Practices Must Truly Be Voluntary.

Any government activity along the lines suggested by the *Request* must be limited to the development and promotion of a *voluntary* set of best practices to deal with botnets or other cyber threats. Voluntary programs have a key advantage over mandatory rules: flexibility. Technology and the associated threats change too fast to address through a formal regulatory process. New technologies, such as implementation of DNSSEC and IPv6; new developments in end user use of Internet content, applications, services, and devices; and new tactics and strategies deployed by the botnet developers and operators,

may have significant ramifications for industry counter-measures and may require a degree of flexibility of response not possible under a regulatory compliance regime.

Voluntary programs would also be consistent with the President's commitment to regulatory humility and to limiting the burdens associated with unnecessary regulation. As President Obama first recognized in January and reaffirmed in July, the regulatory system should "promot[e] economic growth, innovation, competitiveness, and job creation . . . .[and] use the best, most innovative, and least burdensome tools for achieving regulatory ends."[5] To further those interests, the federal agencies must "adopt a regulation only upon a reasoned determination that its benefits justify its costs" and "tailor its regulations to impose the least burden on society, consistent with obtaining regulatory objectives, taking into account, among other things, and to the extent practicable, the costs of cumulative regulation."[6]

Moreover, private entities are likely to share pertinent experiences and data more freely if there is no threat that the information would be used against them to impose regulatory obligations. Voluntary programs would also help promote innovation by enabling participants to focus resources on a wide range of potentially productive countermeasures.

Finally, the government must ensure that regulation in other areas does not constrain the flexibility required by ISPs and other Internet ecosystem participants to engage in activities intended to address cybersecurity threats. For instance, fear of violating the FCC's new net neutrality regulations for blocking access to specific Internet

---

[5] *See* President Barack Obama, Executive Order 13563 (Jan. 18, 2011), 76 FR 3821 (2011) ("*January Executive Order*"); *and* President Barack Obama, Executive Order 13579 (July 11, 20110), 76 FR 41857 (2011) ("*July Executive Order*").

[6] *January Executive Order* § 1(b); *see July Executive Order* § 1(c).

content, applications, and services could cause ISPs to refrain from using certain anti-botnet tactics.

B. ISPs Should Have the Flexibility To Adopt Cost-Effective, Innovative Solutions.

ISPs are keenly focused on protecting their networks from cyber threats. For example, Verizon maintains honey-pot systems, spam-trap systems, and other such systems to detect and track botnet across its global network and the Internet more broadly. Verizon has the ability to identify infected end user machines and the command and control infrastructure for the botnets. Verizon, like other major network providers, can also take action in response to specific threats to sinkhole (i.e., redirect) DNS queries; null-route IP addresses; and block traffic on specific ports and protocols.

Verizon also offers a range of mitigation assistance to its consumer and enterprise customers. Verizon offers technical support services that consumers could purchase for assistance in dealing with a wide range of PC support issues, including botnet remediation. On the enterprise side, Verizon's Forensics and Incident Response team provides 24x7, sophisticated cybersecurity services to assist enterprise and government customers in assessing and addressing cyber intrusions and other threat activity.

Moreover, even without government prodding, market-forces are already moving ISPs in the direction of offering botnet detection and notification capabilities. Verizon offers services in this area to its enterprise customers and is working on initiatives suitable for consumer broadband customers. Verizon Wireless currently provides botnet information to its customers. A range of vendors, including Damballa, Kindsight, and others are offering creative technical solutions in this space for deployment by ISPs. A

flexible approach – rather than mandated rules – would provide an incentive for ISPs and other entities to continue the anti-botnet efforts that they are currently undertaking.

A flexible approach would also allow private entities to mitigate the costs incurred to combat cyber threats such as botnets. Designing systems and processes to notify customers and provide them with tools for remediation is likely to be expensive. There is no reason why the costs should be borne by ISPs. The *Request* appropriately recognizes that government assistance, such as support for a consumer help-desk, may be an appropriate part of the solution.[7] Likewise, various legislative proposals on cybersecurity have proposed accounting and tax incentives to help reduce industry costs.

In today's economy, consumers may be reluctant to incur additional costs. Verizon, like many ISPs, already offers software-based security solutions to its subscribers for a nominal monthly fee, and end users may feel that they have done their part by purchasing antivirus or firewall software. Consumers may not be inclined to take any further steps to protect their machines or clean up an infection. Moreover, some consumers could even view information provided by their ISP on for-fee remediation services as a thinly-veiled attempt to market additional services.

Because cybersecurity technologies can be leveraged for the provision of non-cybersecurity-related services, the revenue from those services could be used to defray the costs of the cybersecurity technology platforms. Technologies, such as protocol analysis, might be well-suited to targeted detection, better enabling ISPs to avoid false positives and implement timely, targeted responses as a result of review of routing or technical information buried in various layers of the protocol stack (e.g., URLs found in

---

[7] *See Request* at 58468.

application-layer header information). Cybersecurity often involves automated collection and processing of vast amounts of communications-related information to find the "needle in the haystack" that is indicative of an advanced persistent threat, a new, fast-moving threat, or vulnerability to information systems and networks.

Separate and apart from their cybersecurity function and with appropriate consent of subscribers, these technologies could also be suitable for delivery of non-cybersecurity services like online advertising. Advertising-based revenue streams have long supported beneficial content, applications, and services on the Internet. ISPs and others should have the flexibility to develop innovative and cost-effective solutions that would be available for those end users who wish to participate in such a program. Legislative or regulatory mandates in the name of privacy that ban or unduly restrict such solutions would have a detrimental effect on innovation that would better secure networks.[8]

Finally, ISPs should have the flexibility to determine how to protect their networks from infected users who refuse to, or are incapable of, cleaning their machines. There are various options in this regard, including suspending or limiting service by the ISP (i.e., establishing a "walled garden") or making the state of infection known broadly enough for individual Internet content, application, and service providers to take appropriate protection to reduce fraud and further infection. An inflexible, one-size, fits-all approach is untenable. For instance, the suspension of service may be effective in

---

[8] For example, in Japan, the Cyber Clean Center's report, "The Fight Against the Threat from Botnets," notes that disrupting communications between a command-and-control server and a botnet is not possible because it "is an infringement of the confidentiality of communications under Japanese law." Section 2.3.1(2), at 5, https://www.ccc.go.jp/en_report/Report_on_the_activities_of_the_Cyber_Clean_Center.pdf (Aug. 31, 2010).

some cases, but in others, it may adversely affect in-home medical monitoring, security cameras, or VoIP services for 911.

C. The Government Should Not Presume That the Best Approach To Combating Botnets Involves Customer Notification by ISPs.

For any given botnet threat, a range of response options exist, including (a) implementing network-based mitigation and notifying end users; (b) implementing network-based mitigation but not notifying end users; (c) notifying end users through one or more means but not implementing network-based mitigation; and (d) doing nothing.

Customer notification raises challenging issues and may not be the most cost-effective way to deal with botnets. It may not be possible, nor even desirable, to notify every end user of every botnet infection. ISPs' resources may be more effectively used to detect and prevent botnets from harming the network.[9] For example, knocking down the botnet early and notifying a handful of infected users are far better than letting the malware infect millions of users and then coordinating a massive notification effort. ISPs should not be forced into one single approach, even if the approach is voluntary and not required by law. Rather, ISPs should have the flexibility to make these determinations based on what makes sense for their networks and business.

Moreover, notification is not solely within the purview of ISPs. ISPs may have a role in translating IP address usage at a particular date and time to a particular subscriber and may possess contact information for that end user, such as a phone number of record, a mailing address, and less-often, a valid email address. Yet that does not necessarily

[9] Indeed, a recent SANS Institute study indicates that ISPs that participated in Australia's voluntary customer notification program (icode) failed to achieve a significant reduction in botnets. *See* Comments of Alan Paller, Director of Research, SANS Institute (Nov. 6, 2011).

mean that the ISP is the best entity to deliver notification of the fact of a botnet infection to the end user.

Because end users have a wide range of relationships with various members of the Internet ecosystem, Internet content, application, or service providers other than the end user's ISP may be better situated to deliver an effective notification that spurs action by the end user.[10] For example, a user about to engage in online banking or e-commerce and enter sensitive financial information might react swiftly to a webpage that notifies the user that the IP address she is using was recently associated with botnet activity at a particular earlier time.[11] This real-time alert may help address instances where a PC is shared by multiple users, but only the subscriber-of-record receives notification. As a complement to real-time notification, an online banking or e-commerce website could take additional anti-fraud (and consumer-protecting) measures as well. For instance, the website might decide to impose an additional waiting period on funds transfers initiated from an IP address known to have just engaged in botnet activity, or otherwise limit

---

[10] Japan's Cyber Clean Center data suggests that spurring consumer action is a challenge as the rate of downloading of disinfection tools by notified end users is low – around 30%. *See* January 2011 activity report (https://www.ccc.go.jp/en_report/201101/index.html) (32.5%); January 2010 activity report (https://www.ccc.go.jp/en_report/201001/index.html) (31.3%).

[11] Verizon offers a service to enterprise customers that might be adapted by online businesses to notify their customers in such instances. Verizon's service provides enterprise customers with the ability to send Verizon the IP address of a machine seeking to establish a connection and nearly instantaneously receive detailed information as to whether Verizon's honey-pots and other security systems observed that IP address to be engaged in botnet-related or other malicious online activity in the recent past, and if so, when and what activity. This service is not limited to just IP addresses used by Verizon's consumer broadband customers, but rather reflects potential malicious activity from any IP address on the Internet. Enterprise customers can then make a decision in real-time as to whether to enable that connection to be established, and if so, what level or range of services to offer that connecting machine at that time.

website functionality for visitors using such an IP address in a manner that might encourage timely end user remediation activity.

Finally, the government could provide an alert or notification to visitors to government websites. The government has various sources of information on bot-infected end points, including Einstein 2, which is an intrusion detection system developed by US-CERT. The government should leverage the vast data gathered by these sources to the benefit of end users and the networks as a whole, rather than use the data solely for the protection of government facilities. As with non-ISP websites, the government's role in the notification and remediation processes may result in more attention and a more appropriate response from certain end users. Because such a notification would come from a trusted, non-commercial, government source, some end users might have a higher comfort level that the information is correct and that remediation is in fact necessary.

III. The Government Should More Effectively Promote Cybersecurity Education.

An educated, prepared, and proactive end user base is a key part of our nation's defense to the botnet threat. End users must develop a sophisticated awareness of the threats posed by activities in cyberspace and exercise good judgment while online.

The *Request* recites the various educational programs offered by DHS, including the National Cybersecurity Awareness Month and the Awareness Campaign "Stop. Think. Connect."[12] While DHS's awareness campaigns are a promising start, much more education should be pursued. The government should significantly enhance its consumer-focused education efforts to the point where cybersecurity awareness

[12] *See Request* at 58467.

campaigns are as ubiquitous as previous successful public education campaigns for seat belts, bicycle helmets, and forest fire prevention. Today, many consumers may be vaguely aware of cybersecurity, but have only a limited understanding of the steps they should take to protect their PCs or the value of purchasing security software. Moreover, the government should particularly emphasize educating school-aged children who are just starting to use PCs and hand-held smart devices to connect to the Internet. Children can adopt security habits that will prove useful – both to them and the networks they use – throughout their lives.

To supplement the government's educational efforts, the private sector should also offer educational resources. Verizon helps support a range of online resources aimed at educating consumers about a wide range of cyber-threats, including botnets.[13] In the enterprise space, Verizon publishes annually its free "Data Breach Investigation Report (DBIR)."[14] Verizon also makes available its Enterprise Risk and Incident Sharing framework to enterprises and government entities to help them share the key facts about security incidents.[15]

IV. The Government Should Facilitate Information Sharing.

A number of outdated laws, including elements of the Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510-22, and various state and local laws, present barriers to the collection, use, and sharing of information by network operators and their customers, and the government. Today's laws may prohibit providers from sharing

---

[13] *See, e.g.*, http://www.staysafeonline.org/; http://onguardonline.gov/; and http://www.netsmartz.org/Parents; *see also* http://forums.verizon.com/t5/Verizon-at-Home/Keep-the-Internet-Safe/ba-p/354691.

[14] *See* http://www.verizonbusiness.com/Products/security/dbir/.

[15] *See* https://www2.icsalabs.com/veris/

certain information that would be invaluable to a provider's defense against cyber attacks. This patchwork of laws needs to be updated so that there is a coherent legal framework that takes into account the current state of technology and strikes the appropriate balance between privacy and the need for information sharing among the government and the private sector.

For instance, Congress should clarify ECPA and the Wiretap Act, 18 U.S.C. § 2511, to encourage providers to share with the government or other network providers the contents of a wire or electronic communication, a stored communication, or customer records for cybersecurity purposes. Congress should also explicitly preempt any other federal, state, or local law or rule. In doing so, Congress should confirm that providers remain free to use customer information gathered for cybersecurity purposes to provide additional, non-cybersecurity services to customers so long as the provider has obtained the appropriate consent of the customer.

In addition to removing potential legal barriers to information sharing, the government should encourage more participation by private entities by limiting the dissemination by the government of information that is submitted. Private entities may be less inclined to share information with the government if that information could be used outside the immediate cyber threat detection and response context. For example, ISPs could be reluctant to participate fully in an information sharing program if the government recipient of the information could share it with other government entities, including Congress and the FCC, that may use that information to justify efforts to impose regulation on ISPs or in enforcement actions targeting ISPs. Accordingly, the

government, with input from the private sector, should develop appropriate protective mechanisms for information shared by private entities.

Finally, information on cyber threats should flow both ways. The government should be willing to share relevant cybersecurity information it collects with ISPs. Specifically, the government should disseminate information on threats and PCs infected with particularly harmful bots to help ISPs prioritize response efforts to protect their networks. To facilitate this sharing, the government should avoid over-designating information as "classified." As noted above, to eliminate any concern about the misuse of government-originated information, the government, with input from the private sector, should develop appropriate protective mechanisms for data that is shared.

V. The Government Should Prioritize Law Enforcement and International Coordination.

The government has a unique role to play in law enforcement and international affairs. The government should prioritize enforcing existing criminal laws against cyber criminals. Moreover, the government should seek to publicize such efforts. Not only would this have a significant deterrent effect, but it would also help educate the public about the importance of protecting themselves from cyber criminals.

Furthermore, the government should work with other countries to eliminate safe-havens for cybercriminals and to ensure a consistency of approach across national boundaries. Botnets know no boundaries. They can migrate from country to country, and botnets that reside abroad can still target U.S. infrastructure. As a result, international coordination is essential.

CONCLUSION

To best promote cybersecurity, the government should ensure that any solutions are developed with all industry stakeholders and that they do not restrict the ability of the private sector to respond to any threat. Verizon welcomes the opportunity to work with the government on a collaborative basis to better secure the nation's networks against the threat of botnets.

Respectfully submitted,

Michael E. Glover
Of Counsel

Mark J. Montano
1320 North Courthouse Road
9th Floor
Arlington, VA 22201
(703) 351-3058

John T. Scott, III
1300 I Street, N.W.
Suite 400 West
Washington, DC 20005
(202) 589-3740

Attorneys for Verizon and Verizon Wireless

November 14, 2011