Before the
United States Department of Commerce
and
United States Department of Homeland Security

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

Response of Microsoft Corporation to Request for Information

J. Paul Nicholas
Senior Director
Trustworthy Computing
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
(425) 882-8080

November 14, 2011

EXECUTIVE SUMMARY

The Departments of Commerce and Homeland Security rightly express concern over the potential economic damage done by botnets and malware. Microsoft is committed to working with its industry and government partners to reduce the impact of botnets and other malware on the Internet ecosystem. We are pleased to provide this input concerning whether there are tools or processes that could, on a national scale, help mitigate the detrimental effects of botnets and malware.

Botnets are a complex problem that requires a multi-faceted global solution. As such, no one entity can solve the problem alone. Microsoft believes that voluntary efforts to combat botnets must include members of the entire ecosystem, as our own experience reflects successful partnership with ISPs, academia, other infrastructure providers, CERTs, and legal counsel. In fact, the most interesting and effective solutions will come from the partnerships between different parts of the ecosystem.

Many members of the ecosystem are already taking significant action to help protect consumers from botnets and malware. Many of these private sector efforts are just now blossoming should be allowed to evolve and grow at the necessary rate to match rapidly advancing threats. Microsoft believes that continued experimentation through practical pilot projects will be most likely to reveal the most effective solutions to this complex problem.

Microsoft places heavy emphasis on the need to disrupt and ultimately prevent botnets in the future. It is important not to simply build mechanisms by which botnet infections can be cleaned up very efficiently, in perpetuity. To do this, we must disrupt the botnet business models by simultaneously raising the attackers' costs while lowering their gains.

Microsoft applauds the Departments for raising the profile of the many important issues addressed in this Request for Information. We hope that this helps to accelerate the many discussions, pilots and decisions necessary across the ecosystem to advance consumer botnet notification models. Microsoft looks forward to continued engagement with government and industry and would welcome any request to discuss these matters in more detail.

TABLE OF CONTENTS

Before the
United States Department of Commerce
and
United States Department of Homeland Security

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

Response of Microsoft Corporation to Request for Information

Microsoft Corporation ("Microsoft"), by its undersigned representative and pursuant to Federal Register notice, 76 FR 58466 (September 21, 2001), hereby submits its comments in response to the Request for Information ("RFI") issued by the United States Department of Commerce's National Institute of Standards and Technology ("NIST") and National Telecommunications and Information Administration ("NTIA") and the United States Department of Homeland Security's National Protection and Programs Directorate ("NPPD") in the above-captioned matter.[1]

I. INTRODUCTION AND BACKGROUND

In the RFI, the Departments rightly express concern over the potential economic damage done by botnets and malware and seek input concerning whether there are tools or processes that could, on a national scale, help mitigate the detrimental effects of botnets and malware. The RFI poses a wide array of relevant questions across a range of issues related to botnet mitigation, but it chiefly focuses on (1) the relative merits and possible approaches to establishing a voluntary code of conduct to aid in this area, and (2) the value of, and possible models for, "a centralized consumer resource center" to facilitate private sector actions to combat botnets.[2]

Botnets and malware are global problems that must be addressed, and Microsoft applauds the Departments' effort to draw attention to this critical issue and to seek workable solutions to the problem. However, the RFI omits any account of the

[1] Hereinafter, NIST, NTIA, and NPPD, will be referred to collectively as "the Departments." By further Federal Register notice, 76 FR 68160 (November 3, 2011), the Departments extended the deadline for submission of comments until November 14, 2011.

[2] RFI, 76 FR 58466, 58467-68 (September 21, 2001).

significant private sector-led efforts already underway in the United State to address many of the very issues the RFI raises.[3] This background is essential to place the Departments' inquiries in the appropriate context. Microsoft is pleased to be able to contribute this input.

The RFI observes that "[c]ompanies and consumers may be able to voluntarily address some of these issues, but to fully address the problem, they will need to work together to clean and better protect computers."[4] Microsoft strongly agrees. Working closely with our partner Internet Service Providers ("ISPs") and members of other sectors, Microsoft has been deeply involved in the campaign against botnets and malware for several years, and together we have gained critical experience from several key efforts against botnets.

Microsoft has a three pronged approach to diminishing the effects of botnets.

First, we work to make Windows a hostile environment for botnets through reducing the attack surface, making exploits less reliable and decreasing the window of opportunity for attack. Additionally, we build anti-malware technologies to prevent and remove infections. Securing the platform helps to raise attackers' costs as they must invest more to develop exploits and have a short period of time to recover that investment. Second, when criminals are abusing our platform or brands we will use legal process to deprive them of that opportunity. These efforts also seek to remove attackers' access to infrastructure such as the domain name system and the computers they have infected, thereby reducing the benefit they derive from these resources. Third, we catalyze ecosystem collaboration to amplify the reach of our efforts. To do this we leverage our global network of partners to share actionable information to enable additional disruptive actions and to assist victims.

II. MICROSOFT'S SPECIFIC EXAMPLES OF SUCCESS: BOTNET TAKEDOWNS AND MITIGATIONS

We have leveraged technical tools in the fight against botnets, and interestingly, we have been able to use the legal system to facilitate the fight as well. These successful operations have the ability to scale globally and can be repeated by motivated parties across the industry and by the government itself.

In February 2010, Microsoft collaborated with VeriSign to shut down the Waledac botnet. Leveraging legal process in a novel approach, Microsoft obtained an *ex parte* temporary restraining order ("TRO") from the U.S. District Court for the Eastern District of Virginia against Internet domains used as connection points for the command and control servers for Waledac and the bots under its control.[5] Under the authority of the TRO, VeriSign – as

[3] The RFI does, however, request descriptions of "scalable measures parties have taken against botnets" and other information concerning them. *Id.* at 58468, question 9.

[4] *Id.* at 58467.

[5] *Microsoft Corporation v. John Does 1-27, et. al.*, Civil Action 1:10CV156 (LMB1UFA).

the registry operator for all .com domains – severed the domains in question from the Internet. With this action, the known connections between Waledac's central command and the individual computers previously under its control were largely severed, thereby decapitating the botnet and disrupting its spamming operations. Once the botnet was disrupted, Microsoft was able to provide IP addresses of infected computers to ISPs and CERTs around the world to enable notification of impacted customers. We have observed that the number of computers infected with Waledac has been reduced by nearly 90 percent from an initial count of approximately 80,000 infected devices since the takedown operation. This operation served as a proof of concept for both the legal and technical actions and has helped to build the international partnerships to assist in notifying impacted users.

Building on this success, earlier this year, Microsoft joined with industry, academic, and international partners successfully to take down the larger, more notorious and complex botnet known as Rustock.[6] This botnet was estimated to have approximately 1.3 million infected computers operating under its control worldwide and was been known to be capable of sending billions of spam mails every day, including fraudulent lottery scams and offers for fake, and potentially dangerous, prescription drugs. Following this operation, we partnered with an even larger group of ISPs and CERTs around the world to notify impacted customers. As a result of this operation, the number of computers infected with Rustock dropped by over 75 percent in 6 months.

Microsoft is also supportive of similar efforts that are led by third parties. For example, when the FBI led the takedown of the Coreflood botnet in April 2011 Microsoft assisted by releasing a special update to the Malicious Software Removal Tool ("MSRT"), which removed the malware from the infected machines.[7]

[6] *See* Taking Down Botnets: Microsoft and the Rustock Botnet, available at http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/03/17/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx ("[N]o single company or group can accomplish this lofty goal alone. It requires collaboration between industry, academic researchers, law enforcement agencies and governments worldwide. In this case, Microsoft worked with Pfizer, the network security provider FireEye and security experts at the University of Washington. All three provided declarations to the court on the dangers posed by the Rustock botnet and its impact on the Internet community. Microsoft also worked with the Dutch High Tech Crime Unit within the Netherlands Police Agency to help dismantle part of the command structure for the botnet operating outside of the United States. Additionally, Microsoft worked with CN-CERT in blocking the registration of domains in China that Rustock could have used for future command and control servers.").

[7] In addition to these recent takedown operations, Microsoft invests heavily to prevent and mitigate botnets around the world. Some of our efforts include: (1) providing security updates to over 700 million computers every month through the Windows Update service; (2) cleaning millions of infected computers each month automatically with the MSRT; (3) providing Microsoft Security Essentials, an anti-malware solution, at no cost to consumers; (4) blocking over 1.5 billion attempted malware installations with the SmartScreen filter in Internet Explorer 8 and 9; and (5) investing in security technologies in Windows such as data execution prevention ("DEP") and address space layout randomization ("ASLR") that reduce the likelihood of successful exploitation of vulnerabilities.

Similarly, Microsoft has been actively involved in anti-botnet efforts within the Messaging Anti-Abuse Working Group ("MAAWG").[8] One of the lessons learned from the take down activities described above is that a lack of standard metrics for measuring the effectiveness of efforts to clean up infected computers creates a disincentive for ISPs to share information about their efforts. To address this problem, MAAWG, leveraging its success in the SPAM/e-mail metrics area, has established an initiative to explore reporting metrics for botnet cleanup efforts.

With regard to measuring the success of efforts to fight botnets, the Departments ask what baseline measurements are available.[9] There are several measures of botnets, malware and infected PCs today ranging from reports by individual vendors to projects such as the Composite Block List[10]. The lack of a commonly accepted view of the problem can make it difficult to evaluate possible solutions and measure success.

To produce a consistent measure of infection that can be used to compare different populations of computers to each other, Microsoft reports infection rates using a metric called *computers cleaned per thousand,* or *CCM,* which represents the number of computers cleaned for every 1,000 executions of the Malicious Software Removal Tool ("MSRT"). The MSRT data is used because the tool's global reach, large installed base, and regularly scheduled release facilitate the comparison of relative infection rates between different populations of computers.

Microsoft's data, while immense and global, is limited to computers running the Windows operating system. As malware targets other operating systems as well, this is not a complete view of the problem but a reasonable proxy. We do also caution that there are a myriad of reasons for changes in the measurement of botnets and infected devices. Accordingly, it is difficult to determine the actual causes of these changes. Microsoft is actively engaged in the Federal Communications Commission ("FCC") Communications Security Resiliency and Interoperability Council ("CSRIC") working group 7 chartered with addressing this specific issue.

While still maturing, collectively, the efforts described above demonstrate that the very sort of voluntary, collaborative, broad-based private sector-led framework for botnet mitigation envisioned in the RFI is already developing and taking hold in the U.S. They also illustrate how such an industry-led approach to botnet disruption, notification, and mitigation can be most responsive to consumer needs while keeping pace with ever evolving online threats. As the MAAWG example illustrates, while answers to many of the logistical, technical, and business challenges in this area remain unclear, industry is

[8] http://www.maawg.org/ MAAWG brings together a broad cross section of members of the messaging industry "to work collaboratively and to successfully address the various forms of messaging abuse, such as spam, viruses, denial-of-service attacks and other messaging exploitations. To accomplish this, MAAWG develops initiatives in the three areas necessary to resolve the messaging abuse problem: industry collaboration, technology, and public policy." http://www.maawg.org/about_maawg.

[9] RFI, *supra* note 2, at 58469, question 13.

[10] http://cbl.abuseat.org/

independently and purposefully grappling with them to find solutions that work across the diverse landscape of interested stakeholders. These efforts should be encouraged and allowed to continue. As the Departments proceed in this area, they should do so cautiously to avoid disrupting this emerging framework.

III. DISCUSSION

A. A Voluntary Code of Conduct Would be Premature at this Juncture, and Industry has Demonstrated the Ability and Willingness to Make Progress in this Area Without One.

The primary inquiry presented in the RFI concerns "the requirements of, and possible approaches to creating, a voluntary industry code of conduct to address the detection, notification and mitigation of botnets."[11] The Departments also ask about preventative measures that could help to stop botnet infections before they happen and specifically ask whether there would be any "benefits to developing and standardizing these practices for companies and consumers through some kind of code of conduct or otherwise?"[12]

Identifying existing and developing new codes of conduct cannot be successfully accomplished without first understanding the security goals and objectives the government and private stakeholders are trying to reach and behaviors and outcomes that are desired or necessary to accomplish them. Together, these objectives and outcomes lead to risk management principles that can form the basis for voluntary codes of conduct. While the security goals and objectives associated with botnet mitigation may be relatively clear, the required behaviors are not.

As noted above, industry's experience with botnet take down and clean up in the Waledac and Rustock cases has yielded further questions concerning the technical, logistical, and business case requirements that are still being explored. Accordingly, at the present time, the necessary elements of a "code of conduct" remain unclear. While important progress is being made, this area is not yet mature enough for formal standardization. Continued experimentation through practical pilot projects, not formal standards, will be more likely to reveal the most effective solutions to this complex problem. In lieu of formal standards, we suggest that industry focus on adoption of best practices and consistency in approaches where appropriate, in particular looking for ways to apply techniques similar to Microsoft's use of the legal system to facilitate botnet takedowns. As they begin to emerge, common (though not prescribed) approaches will reduce user confusion and help more members of the ecosystem adopt these important practices.

Moreover, the RFI appears to presuppose that a voluntary code of conduct is necessary for action in this area. However, as the case studies outlined above evidence, this is not the

[11] RFI, *supra* note 2, at 58467 (Summary).

[12] *Id.* at 58468, questions 2-3.

case. Industry action is moving forward notwithstanding the lack of a clear code of conduct. Indeed, it is such industry activity that may ultimately yield a clearer picture of what such a code should look like.

Additionally, Microsoft acknowledges the Departments' request for input on providing incentives for entities to participate in efforts to defeat botnets. However, for the same reasons just noted, the processes and drivers for action are still emerging. Thus, the most effective market or technical incentives to drive action remain unclear. In addition, while the Departments can and should continue to encourage the government, and private sector companies, to use legal process to take down botnets, it is not clear that any government incentive is needed.

B. An Industry-led Approach with Distributed Responsibilities Provides a Balanced Model for Fighting Botnets Now and in the Future

The second major focus of the RFI concerns the value of, and possible models for, "a centralized consumer resource center" to facilitate and incentivize private sector actions to combat botnets.[13] The RFI presents three possible scenarios for such a center – private sector run and supported; public/private partnership; government run and supported – and asks a series of questions concerning the relative merits and possible requirements of each of the models.[14]

Microsoft believes that industry and government in the U.S. and around the world should collaborate to improve and maintain the security of devices on the Internet. Every member of the Internet ecosystem has a role to play in protecting consumers against online threats such as botnets and related malware, including consumers themselves. The unique role each plays depends on the relationship they have with the consumer and their ability to determine that a particular device is infected with malware and mitigate its impacts.

Private sector companies in the United States and around the world are currently engaged in a variety of efforts to both disrupt botnets and to notify and remediate infected consumers. Microsoft's own efforts, detailed above, have yielded positive results and valuable experiences that should be replicated globally. Although this work is not yet to scale, it would be premature for government to intervene with any centralized operational services. The business case for such a function does not yet exist.

Microsoft has studied the efforts against botnets in Australia, Germany and Japan, among others. Microsoft is actively participating in the FCC CSRIC working group 7 that is further examining these international efforts. It is clear that there is no "one size fits all" approach to fighting botnets at a national scale. We do note that in several of these

[13] *Id.* at 58467-68.

[14] *Id.* at 58469, questions 25-30.

cases the government programs preceded private sector efforts. In the United States the private sector is already leading the way. The activities underway reflect the principle that effectively combating botnets requires broad-based collaboration among a range of interested stakeholders. However, it is the nature of such collaboration models that they start with a well-defined group of participants who can pilot and prove what approaches work best, and grow to scale with experience and greater maturity. Centralizing these programs could disrupt existing work and could stifle new activity.

Successful efforts against botnets require technical knowledge of the affected technology (online services, operating systems and networks) and a trusted relationship between the service provider and the consumer. The private sector companies who provide these services possess both the technical understanding necessary to disrupt botnets and the trusted relationship with consumers. Adequately addressing consumer security online requires careful attention be paid to both the evolution of threats and the ever changing online usage patterns of consumers. The private sector is best positioned to understand and react to both of these demands.

Moreover, it is also important to recognize that the current efforts against botnets represent just a baseline of what is needed to effectively protect consumers. As set forth more fully in section C below, Microsoft believes that additional efforts to protect consumers, while building on the existing foundation, should be distributed throughout the ecosystem. This approach cannot be implemented effectively in a centralized manner. Establishing a center enables the transfer of responsibility and creates the risk of a moral hazard. In addition relying on a center also creates challenges that include yearly funding, organizational governance and accountability, and potentially obsolescence.

Private and public sector entities are actively collaborating in the fight against botnets. Undoubtedly, we are in the early stages of this battle and all members of the ecosystem must continue to innovate and collaborate in order to disrupt, mitigate and ultimately prevent bots. As no one entity can succeed alone, Microsoft's view is that we must continue to embrace a distributed approach where each member of the ecosystem fulfills the role for which they are best suited. The government can play a valuable role in facilitating and enabling these efforts, but the operational and technical aspects are best led by the private sector entities that have the closest relationships with the impacted customers.

C. Efforts to Disrupt, Mitigate and Protect Against Botnets Need to Involve the Entire Ecosystem, not just ISPs

The RFI recognizes that, to date, most government attention in the botnet area has been devoted to the potential role that ISPs can play.[15] The Departments ask whether this focus on ISPs is appropriate or whether other entities can also participate in botnet

[15] *Id.* at 58469, question 12.

mitigation efforts.[16] Botnets comprise a complex problem that requires a multi-faceted global solution. As such, no one entity can solve the problem alone. In fact, the most interesting and effective solutions will come from the partnerships between different parts of the ecosystem. Microsoft believes that voluntary efforts to combat botnets must include members of the entire ecosystem, as our own experience reflects successful partnership with ISPs, academia, other infrastructure providers, CERTs, and legal counsel.

ISPs do have a unique role in helping to defeat botnets. ISPs are, in effect, the only entities that can identify the impacted customer from an external report which is often limited to just an IP address. Microsoft works with a number of ISPs around the world to notify consumers who have been victims of botnets such as Waledac and Rustock. These ISPs partners have worked to notify their customers of security issues and providing them with helpful resources to help remediate the problem and help prevent it from recurring.

However, while ISPs occupy a unique position, they are not the only entities that need to be involved. Entities including but not limited to operating system and application vendors, security software vendors, domain name services, hosting companies, online service providers (banks, email providers, and social networks), ISPs and consumer organizations can make meaningful and relevant contributions to solving the problem. To be most effective, these other entities should focus on the functions for which they are uniquely suited and that they are best equipped to provide.

For example, operating system and application vendors are best suited to reduce the attack surface of their products and to provide security updates when vulnerabilities are discovered. Anti-malware providers have specialized knowledge of threats and are aptly positioned to produce solutions to block emerging threats and remove infections from devices. This distribution of responsibilities allows for leveraging trusted relationships, specialization of services, and differentiated levels of security depending on the value of the asset at risk. Exploring the full complement of necessary functions and stakeholders is not complete and should be an early focus of voluntary efforts.

D. Notifying Consumers of Malware Infections Would Accelerate Efforts to Defeat Botnets

As noted above, successful efforts to defeat botnets must involve the entire Internet ecosystem, not just ISPs. In our work with them, Microsoft encourages service providers generally to notify customers that they believe to be impacted by malware.[17] Notifying the impacted end users is the first step to help them to disinfect their computer and take steps to prevent future infection. Additionally, the consumer may want to take steps to ensure his or her identity, personal data, or financial information have not been impacted.

[16] *Id.*

[17] *Id.* at 58468, question 7.

The RFI asks whether "notices, and/or the process by which they are delivered, [should] be standardized?"[18] To support effective notifications, industry should work to create a commonly accepted framework for notification characteristics. This framework should cover both the criteria for delivering a notice and the medium by which is it delivered with attention paid to identifying and addressing any legal impediments to contacting an impacted customer. In addition, this framework should address the common information elements that should be included in a notification. This will help improve customer reception of the notices and also help to build defenses against fraudulent notifications and social engineering.

Once notified, consumers can be connected with a variety of existing resources to remediate the malware infection. Today, these resources are provided by Microsoft, anti-virus vendors, ISPs and others. Many of these tools are provided at no cost to the consumer. Consumers can be directed to these resources by their ISP or access them directly from vendor websites. For example, the freely available Microsoft Safety and Security Center located at http://www.microsoft.com/security/ provides information and tools for consumers to remove malware infections and bolster defenses against future threats.

While we are supportive of efforts to notify customers of infected devices, we must recognize the increased possibility for fraudulent notifications. Microsoft suggests that notices delivered to consumers be carefully designed to maximize effectiveness and resist fraud.[19] There are two key aspects to making notifications resistant to fraud and effective to end-users regardless of the form they take. First is to establish a trusted communications channel, so that users can be assured they are getting notifications from a trusted entity, and not just another attacker trying to get them to put malware on their system. Second is to explain the problem and the solution in terms the user can understand and with steps they can easily follow.

The Department of Commerce, through NIST, can help advance the state of notification techniques and effectiveness with comprehensive testing and evaluation of the notification messages, mediums and effectiveness.[20] Microsoft encourages NIST to collaborate with the private sector on this research and broadly share results of these tests so that others can similarly improve their notifications.

With regard to whether or not these notices and the process by which they are delivered should be standardized, Microsoft believes that it is premature to formally standardize notifications to consumers impacted by botnets. Standards seem to work best when there is a concept that is working well and can be described as a defined

[18] *Id.* at 58469, question 15.

[19] *Id.*

[20] Notifications should be tested to see if users understand important elements about them, such as who the notifications are from, why the users are receiving them, what the impact of being infected is, or how to deal with apparent false positives. These efforts should also consider measuring unintended consequences. For example, how many rogue AV infections mimicked official looking notifications? Or, is the public's ability to recognize fraudulent notifications improving?

operation. Notifying consumers impacted by malware is still very much in its infancy. This is a time when industry should be investigating many ideas to find the most effective approach rather than prematurely standardizing an existing approach.

As part of its role to connect consumers with the business community, the Department of Commerce should consider maintaining a listing of entities providing notifications, what those notifications look like and the resources they include. This centralized listing could help thwart user confusion and reduce the risk of fraudulent notifications. When consumers receive a notification, they could consult the listing to help determine if it is legitimate. Separately, if consumers were concerned that they were infected by a bot they could proactively visit this site for information on how to remediate the issue. This listing would be a supplement to, but not a substitute for, the work already underway by various private sector organizations.

E. Current and Future Technologies Can Help Prevent and Mitigate Botnets and Malware Infections

The most effective measure an end user could take to stop botnet infections before they happen[21] would be to use the most current versions of operating systems, applications and security software available to them. Online threats have evolved rapidly and in ways that could not be imagined at the time some products were developed. At the same time, Microsoft and other industry members have continued to make successive versions of products more resistant to attacks.

This fact is demonstrated in Microsoft's Security Intelligence Report.[22] Each successive version of Windows has a lower CCM[23] than its predecessor. For example, Windows 7, the most recent version, has a CCM rate less than half of its predecessor Windows Vista.

Our analysis also shows that the majority of software vulnerabilities are found in 3rd party applications. It is important that consumers keep these 3rd party applications up to date as well. This activity tends to require a higher degree of technical knowledge and there may be an opportunity for commercial solutions to help increase adoption of this practice.

Microsoft and several other software vendors provide anti-malware and remediation solutions at no cost to consumers with high levels of adoption.[24] In addition to removing economic barriers, solutions must be accessible, effective and user friendly. To date, over 30 million consumers have downloaded and installed the free anti-malware solution, Microsoft Security Essentials.

[21] *Id.* at 58468, question 2.

[22] http://www.microsoft.com/sir

[23] CCM is a measure of malware infections removed from computers, described in section II.

[24] RFI, *supra* note 2, at 58469, question 16.

Additionally, Microsoft's Malicious Software Removal Tool (MSRT) runs on over 600 million computers automatically every month as part of the Windows Update process. The users of these computers have opted to have their computers scanned for the most prevalent families of malware and the tool is able to remove any that it finds.

Microsoft recommends that users whose computers are infected with malware[25] run the Microsoft Safety Scanner[26] on their computer. This tool detects and removes all malware known to Microsoft including Waledac and Rustock that were targeted in our recent operations. This tool is available at no cost to consumers and runs on all supported versions of Windows.

Once the infection has been removed, we recommend that the user takes steps to better protect against future infections. These steps are simple and can be performed at no cost to the user. They are to:

1. Enable automatic updates from Microsoft and other trusted software vendors to receive fixes to known security vulnerabilities.

2. Turn on a firewall to block malicious network traffic.

3. Run and keep current an anti-malware solution.

4. Use a modern web browser.

Microsoft places heavy emphasis on the need to disrupt and ultimately prevent botnets in the future. It is important not to simply build mechanisms by which botnet infections can be cleaned up very efficiently, in perpetuity.

F. Successful Efforts Must Also Aim to Disrupt the Botnet Business Model

There are powerful economic forces behind malware and botnets. As long as there is money to be made, the criminals behind botnets will continue to find creative new ways to exploit consumers and business. The primary goal of these efforts must be to make the botnet business unprofitable. To do this, we must disrupt the botnet business models by simultaneously raising the attackers' costs while lowering their gains.

Disruption of botnets has been a major investment on the part of Microsoft. Our view is that we have been quite successful in disrupting botnets to date, and are confident that our internal work reflects a best practice in the fight against botnets.

As noted above, Microsoft's three pronged approach towards botnet takedown and mitigation has been quite successful: (1) evolve technology to withstand threats more effectively; (2) leverage legal process; and (3) partner with others to increase the beneficial

[25] *Id.*, at 58469, question 23.

[26] http://www.microsoft.com/security/scanner

effects of our work. The Department of Justice can be a focal point for disrupting botnets through legal process. Exemplified by the successful takedown of the Coreflood botnet led by the FBI, law enforcement actions do not necessarily need to result in prosecutions to be impactful. The government should work with its law enforcement agencies to incentivize successful disruptive actions even when they do not result in prosecution.

IV. CONCLUSION

Microsoft is committed to working with its industry and government partners to reduce the impact of botnets and other malware on the Internet ecosystem. Many members of the ecosystem are already taking significant action to help protect consumers around the world. These largely private sector efforts are still maturing and should be allowed to evolve and grow in advance of online threats.

Microsoft commends the Departments for raising the profile of the many important issues addressed in this RFI. We hope that this helps to accelerate the many discussions, pilots and decisions needed across the ecosystem to advance consumer botnet notification models. Microsoft looks forward to continued engagement with government and industry and would welcome any request to discuss these matters in more detail.

Respectfully submitted,

J. Paul Nicholas

J. Paul Nicholas
Senior Director
Trustworthy Computing
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
(425) 882-8080

November 14, 2011