BEFORE THE

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
DEPARTMENT OF HOMELAND SECURITY

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

Comments of Electronic Frontier Foundation

The Electronic Frontier Foundation (EFF) is pleased to submit these comments in response to NIST's, NTIA's, and DHS's (collectively, "the Agencies'") Notice of Inquiry dated September 21, 2011.

We agree that botnets are a worrying problem, and one that threatens the privacy and security of individual Internet end-users whose computers are infected as well as the availability and integrity of systems and services that are attacked by botnets. Botnets are making the Internet less safe and we appreciate the urgency of the Agencies' inquiry and many parties' research into how to protect against them.

Broadly, we believe that efforts to warn end-users when their computers are likely infected are desirable and are not typically a privacy problem. As the Agencies and other commenters have recognized, however, warning end-users can be extremely challenging. Many users may not understand the content of the warnings (or their potential significance). And many users are rightly skeptical of e-mailed claims or browser banners that claim that the users need to download software or provide billing information in order to fix a purported security vulnerability. However, we welcome efforts by government or private parties to overcome these challenges.

We are particularly concerned about five measures that ISPs might take in response to the botnet problem:

- ISPs might try to proactively block their users' access to sites and services that they believe are common vectors of botnet infection;
- ISPs might directly monitor and examine their users' Internet traffic to look for signs of an infection (such as participation in an attack, or communication with command-and-control servers);
- ISPs might "quarantine" apparently infected subscribers by temporarily preventing them from accessing the Internet;
- ISPs might try to require subscribers to run particular software or software versions on their personal computers; or
- ISPs might alter the content of third-party web sites by modifying or proxying network traffic, in order to insert warning or notification banners.

All of these measures will be tempting (and all of them have already been tried in some places) because they seem to bring the ISPs' substantial power directly to bear on the problem. However, these measures also significantly alter the nature of the relationship between the ISP and its subscribers and the nature of the Internet access service itself. Some of them also risk affecting the service of users who are not infected at all but who share an Internet link with someone else.

ISPs must be transparent about the botnet control, detection, and notification practices they employ. Botnet-control services that involve blocking, monitoring, or altering users' Internet traffic (apart from blocking an active attack against other parties) should be provided only on an opt-in basis. Measures taken on an emergency basis to stop or disrupt an ongoing attack should also be proportionate and, as far as possible, provide a way for affected users to learn what is happening.

We respond to some of the Agencies' specific questions as follows:

2. Stopping infections before they happen

4. *Preventing and mitigating botnet infections*

Taking a broad interpretation of these questions, we think it's important to highlight that we should be exploring solutions to the botnet problem that involve taking away the incentives for people to build and maintain botnets. Indeed, operating botnets requires significant resources and so understanding the economic and political

motivations for running botnets can go a long way towards solving the botnet problem. In particular, we should look hard at ways to remove any economic gains of running a botnet, for example by increasing the cost of such an operation through increased computer security.

More narrowly, there are many ways in which infections might be prevented, all in keeping with the general theme of increased computer security. For one, software downloads should be provided only over HTTPS. Operating systems should implement security measures such as better sandboxing, and better handling of software downloaded from e-mail attachments. Browsers should improve security as well, and make sure that users are not easily tricked into making bad decisions. With such an improved security ecosystem, we believe it will be much harder to infect computers and hence run botnets.

7. Contacting subscribers when infections are discovered

Contacting subscribers when their machines appear to be infected is appropriate and desirable. However, the effectiveness of notifications of this sort is questionable because users are increasingly appropriately skeptical of e-mail messages (for example) claiming that their computers are infected with viruses, since the majority of such messages are typically scams or spam, and some are themselves vectors for malware infection!

ISPs and other entities should be careful not to begin employing notification techniques that are easily counterfeited or co-opted by malware distributors, or that train users to uncritically take actions that would be dangerous in a similar context (such as installing software from an e-mail attachment or an unfamiliar website).

6. *Data sharing*

10. *Maintaining privacy of personal data*

There are many situations in which we think there is little privacy risk from good-faith information sharing about botnet infections, especially if the information shared consists mainly of reports from abuse victims.

There are important exceptions. For example, if a search engine analyzes log data to find evidence of botnet infections, some of the data it analyzes could involve real user

searches or user identities. A bad result could occur if a search engine miscategorizes some real user search queries as synthetically generated by a botnet as part of spam or other abuse, and then discloses those queries to third parties as evidence of an infection. Similarly, an e-mail provider that tries to identify compromised hosts by analyzing its login records could reveal actual user location information if it misidentifies legitimate user activity as an intrusion and discloses log contents about the "intrusion" to third parties.

All of these privacy risks from investigations into computer intrusions have existed for decades and have been discussed in computer security literature. For as long as computer crime has existed, the process of investigating and countering it has involved some risk of system administrators and others getting inadvertent access to personal information. This is not a new consequence of the botnet problem. However, since today's Internet includes extremely large application service provides with millions of users, the *scale* of this risk is far larger than in the past.

Application service providers that plan to analyze personal data to investigate and counter botnets and other abuse should carefully consider the privacy risks of reviewing and disclosing particular kinds of information, particularly considering how certain they are that particular unusual behavior is truly a result of an intrusion, and should share the smallest amount of personal information necessary to provide convincing and useful evidence of the apparent intrusion.

11. *Avoiding false positives*

ISPs and other service providers should understand that the use and operation of privacy and anonymity services like Tor could result in traffic patterns superficially similar to those of a botnet. They should consider whether they are using any heuristics that could classify proxy use or the use of proxy networks or distributed services as a botnet infection. Even sophisticated heuristics can err, and so it is crucial that ISPs and service providers rigorously measure the false positive rate in whatever classification system they develop, since in the context of sharing information and taking action to message a user, the cost of a false positive is quite high.

12. *The role of ISPs vs. other entities in botnet detection*

We agree with the Agencies' observation that entities other than ISPs may be in a good position to detect (and perhaps even act upon) botnet infections. Entities like search

engines, for example, may be the *victims* of abuse from botnets, so they may be in a good position to see clearly where that abuse is originating from and to find other patterns relevant to understanding the structure and extent of a botnet. From a privacy point of view, they are often better-positioned to detect and analyze botnet activity than ISPs, because the nature of their relationship with users (unlike ISPs') necessarily already involves examining and acting upon the content of traffic delivered to them. As such, we think that botnet detection should primarily be situated with search engines and other large online service providers, and that the role of ISPs should be comparatively small.

14. *Effective notifications to subscribers*

We suspect notifications to subscribers by a non-Internet means such telephone or paper mail will usually be more credible than an Internet means such as e-mail. Since effective notification is so difficult, we hope large ISPs will carry out more experiments with notification techniques and share their results widely.

18. *When users don't respond to notifications*

We are concerned that users' non-response to notifications may be used as an excuse for compelling users to run particular software applications (such as network admission control software) or operating systems, or for quarantining them by blocking their access to the Internet until they take particular actions. These measures are particularly disproportionate and unfair in light of the diversity of devices and operating systems that are used to connect to the Internet and the fact that a single Internet access subscription may be used by a very large number of individuals – only one of whom might be infected, but all of whom could be affected by a quarantine or other measures.

There are also clearly a variety of situations in which enforcing a quarantine would result in far greater harm than allowing an infection to persist.

Conclusion

Although we have a variety of strong concerns about particular measures that might be brought to bear in response to the botnet problem, we agree that botnets are a serious problem and that new and further measures to address it are needed. This

problem is now large and thorny enough that we are not particularly optimistic that it can be resolved any time soon, but we look forward to reading others' comments in response to this inquiry and learning what measures other parties propose.

DATED: November 4, 2011

Seth Schoen
Senior Staff Technologist
<schoen@eff.org>

Dan Auerbach
Staff Technologist
<dtauerbach@eff.org>
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Tel: 415 436 9333
FAX: 415 436 9993