Johannes B. Ullrich, Ph.D
PO Box 13314

• Jacksonville, FL 32206• Phone: +1 (757) 726-7528
E-Mail: jullrich@sans.edu Web: http://isc.sans.edu

Date: November 4, 2011

Public comment in response to the notice:

“Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware”

The detection, reporting and mitigation of large-scale network attacks have been a focus of the Internet Storm Center and DShield ever since their respective inception. The initial work that resulted in building the sensor network and reporting engine behind DShield was prompted by the need to facilitate more effective reporting of these incidents. Since then, many other systems adopted this approach to collect and disseminate information about malicious network activity.

DShield.org, by integrating with the SANS Internet Storm Center, adopted a two tier approach. DShield.org continues to serve as an automated data collection engine, while the Internet Storm Center provides human analysis of the data including the collection of reports by end users who either do not use the DShield system, or are reporting more complex events that do not fit the data model employed by DShield.

During the more then 10 years of collecting and reporting intrusions, botnet infections and other security incidents, we consistently run into two very specific problems making the mitigation and cleanup process slow and inefficient, to the point were we currently send hardly any notices down from several thousand a day a few years ago.

Modern malware spreads on the scale of minutes or hours. Any meaningful response curbing the spread of malware has to happen on a similar time scale. We believe that the only way to achieve a rapid and effective mitigation is to largely automate these systems. Automation is also in the interest of other stakeholders, in particular ISPs, as it will reduce the costs involved in mitigating the infections.

Our most difficult problem is finding an appropriate contact to report the event to. While many large ISPs have well developed “abuse” procedures to deal with reports of infected machines, finding the correct contact can be labor intensive and has turned out to be difficult to automate.

If a contact is identified, the report needs to be formatted in a way that is easily understood and processed by the recipient. The receiving organization needs to be able to correlate reports received from various sources in order to prioritize and filter the reports.

Sincerely,

Johannes B. Ullrich,
Dean of Research, SANS Technology Institute