Before the
DEPARTMENT of COMMERCE
National Institute of Standards and Technology and the
National Telecommunications and Information Administration

And

DEPARTMENT of HOMELAND SECURITY
Docket no. 110829543-1541-01

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

COMMENTS OF SANDVINE INCORPORATED

sandvine®
Intelligent Broadband Networks

SANDVINE INCORPORATED
408 Albert Street
Waterloo, Ontario
Canada
N2L 3V3

November 4, 2011

About Sandvine

1. Sandvine appreciates the opportunity to respond to the Request for Information from NIST, NTIA and DOHS in connection with establishing voluntary corporate guidelines for notifying consumers of potential botnet infections, as published in the Federal Register on September 21, 2011.

2. Sandvine was established in 2001 and employs approximately 450 people in Canada, the United States, Israel, India and in remote offices globally. Sandvine has been named by Infonetics Research as the global market share leader in the "Standalone Deep Packet Inspection market", and has been named multiple times to the Deloitte Technology Fast 500 list of fastest growing technology companies in North America.

3. Sandvine's network policy control solutions make the Internet better by protecting and improving the Internet experience for subscribers. The solutions comprise network equipment and software that help consumer broadband service providers (both fixed line and mobile) understand network traffic and trends, mitigate malicious traffic, mitigate network congestion, protect the quality of experience for sensitive applications, offer subscribers new services, and improve customer service. Specifically in relation to the Request for Information, Sandvine offers a solution for detecting and mitigating botnet infection, and automating communication of the event with the subscriber.

4. Sandvine's technology is used by more than 200 Internet service provider customers in over 80 countries. Together, Sandvine's customers serve hundreds of millions of fixed line and mobile broadband Internet subscribers.

5. In the Request for Information, the NIST, NTIA and DOHS have requested comment on a variety of issues related to handling botnet infections. Sandvine has focused its comments on the technological aspects of the issue as that is where the Company believes it can best contribute to the discussion.

Comments

6. Sandvine believes that the detection of botnet activities is best achieved through a combination of analyzing network traffic behaviour and various application identification techniques. The two techniques in isolation provide limited value when compared with a converged strategy where both the behaviour of traffic is combined with the ability of detecting data packets patterns of interest, which in the context of botnets primarily means tracking traffic according to known Command and Control or infected hosts. A converged strategy limits the opportunities for false positives in botnet detection.

7. There are different mechanisms currently employed in the industry that allow for the implementation of such techniques, but the one that is most relevant to this discussion is the idea of measuring a "vulnerability score" associated with the end user's computer resources.

8. Effective vulnerability scores are calculated based on the analysis of traffic exchanged between end-users and the Internet. Certain traffic patterns are more or less likely to be associated with malicious activity. By combining heuristic analysis of data such as IP packets rate, length, frequency and source/destination with indicative patterns of user's broader exposure to threats,

such as the Operating System Version, Anti-virus signature updates, and other factors, a reliable vulnerability score can begin to be determined. Effective strategies also require flexibility to receive a variety of inputs as part of the scoring model. For example, adding an ability to match traffic source and destination to IP,domain lists and URL lists (commercial or open source) of systems that are known or suspected to be compromised by botnet Command & Control software would add significant value.

9. We believe that a model built around the careful correlation of those two sources of data allow for the assignment of a vulnerability score representative of the real state of the end user systems. A score would be assigned to all network users. To prevent botnet infection to spread, notifications towards the user could begin as soon as the score reached a predetermined critical threshold level and potentially in advance of a detected infection. The components of the score (old operating system, communication with high risk servers, etc.) could be communicated to the user to help them reduce risk and lower their vulnerability. To optimize privacy, score components would not be revealed as part of the user's account records until the threshold level was reached and communication became necessary for network integrity.

10. We strongly support proactive subscriber notification as a mechanism to enforce and instil accountability to all stakeholders involved in the process. Whether the notification relates to communication regarding enhanced vulnerability or of an actual infection event, effective notification systems need these attributes:

    i. Timing – real-time notifications are most effective in limiting the spread of malicious traffic, just as they are most effective in addressing other network concerns, such as bill-shock notification.
    ii. Media – notifications may require a different medium according to individual situations and those should include technologies such as real-time advice through a web page, SMS, email, Smartphone apps and other techniques that allow not only for a message to be sent on time but at the correct "device and location". Aspects such as user mobility and multi-internet-screens at home require different delivery strategies for an effective communication.
    iii. Personalization – allowing users to control their notification preferences can help with accountability and empowerment instead of a fixed "one size fits all" approach. Personalization should come in the way of allowing users to configure their preferred notification media and also in terms of providing user options when the notification is received. Additional functions could allow the user to decide whether any suspect traffic should be re-directed or blocked for a period of time.

11. Inaction on the part of the subscriber in reaction to notifications of an infection event or of increased vulnerability could be fed back in as a component of the user's overall vulnerability score.

12. In terms of network installation and placement the most important principle is that the more comprehensive the coverage the better visibility on data enabling higher possibilities for tracking user vulnerability and malicious activities. In other words, deployments should target network segments closer to the subscriber premises as opposed to installing at core (more central) locations. One of the reasons for such is that most advanced botnet systems resort to different techniques for infection and command and control activities including the disguising of

traffic using other well known protocols such as HTTP and several peer-to-peer protocols. Because of the nature of peer-to-peer traffic (which does not reach the core of the network) the systems need to be installed at network segments that allow for greater data visibility (closer to the subscribers). Several challenges arise due of such requirement including the need to support IP encapsulation therefore requiring effective technologies to comply with such requirements.

13. The Request for Information dedicated significant attention to the notion of a centralized consumer resource centre. Sandvine believes that a more robust approach is for individual service providers to implement independent "Notification Center" web portals for educational campaigns, notifications, device cleansing, and personalization adjustments, as described earlier. A centralized approach for notification, as discussed at length in the Request for Information, where all national users are directed to a single location could be more vulnerable to circumvention and exploitation by malware and other types of infections. For example, it would be easier for malicious actors to imitate the appearance of a centralized resource so that it ends up being used as a means for infecting users rather than as an effective tool for cleansing them.

14. A more distributed and diverse approach where different carriers follow basic guidelines of implementation would enable a more robust framework. Providing guidelines for implementation of the notification centers would be valuable and could ensure a minimum level of security and also create a widespread visual identity allowing users to recognize it. The guidelines for implementation should include:
    - Usage of secure sockets layer (SSL) with security certificates associated directly with the service provider
    - Links to government-provided educational resources
    - Live access to a customer service representative, both via chat and voice.

15. The latter is a crucial requirement in order to prevent "scammers" from creating similar pages in order to obtain information or infect user's devices. Guidelines could also be established for the visual techniques used to present the notification messages. There are technologies available today to provide non-disruptive notification messages through visual modes such as the following. The approach could be compared to the communication mechanisms used by airport or other public Wifi services.

    i. Frame insertion - where a specific frame or other element "overlaid" to the page is added to preserve the full context of subscriber's navigation. The frame provides basic information with respect to the situation including links to specific additional information (e.g. the Notification Center).
    ii. Contextual web page redirection – a seamless redirection mechanism that preserves the originally requested URL address allowing the user to continue its browsing experience once the information provided is verified and specific options chosen.

16. There is also value in mandating an audit log of notifications and actions taken by end-users to a centralized government unit although privacy concerns need to be carefully addressed. The value of a centralized view of subscriber's "vulnerability scores" combined with the notification entries and actions taken could be used to identify infection spreading patterns and also other types of illicit activities, strengthening the industry's ability to deal with the growing capabilities of botnets. Conversely, the logs could be maintained by service providers and forwarded to a

centralized government unit when deemed critical by government due to broader increased risk levels.

17. Some of the international cases mentioned offer central agencies and service providers the ability to select specific subscribers to be notified of botnet infections. Basically the idea where a centralized agency provides a list of infected IP addresses to the service provider that could immediately become a source of notification to end users is another critical requirement analogous to EAS (Emergency Alert System) type of services. Systems should be capable to receive lists provided by central agencies with specific notification severities and/or instructions associated with it.