

BITS

FINANCIAL SERVICES
R O U N D T A B L E

Filed via online portal Consumer_Notice_RFI@nist.gov

November 14, 2011

National Institute of Standards and Technology at the
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4822
Washington, DC 20230

RE: Docket No. 110829543-1541-01

To Whom It May Concern:

BITS¹, the technology policy division of the Financial Services Roundtable, appreciates the opportunity to provide comment to the Department of Commerce's (Department) Request for Information regarding "Models to Advance Voluntary Corporate Notification to Consumers Regarding the Illicit Use of Computer Equipment by Botnets and Related Malware."

BITS members are concerned about botnets and malware impacting our customers, and strive to do everything that can be done to protect them from such attacks, including making the online banking channels extremely secure. The financial services industry is a primary target for malware-enabled cyber attacks. Cybercriminals directly target financial institution customers and business partners using malware-enabled attacks. BITS released a paper in June 2011 (attached) to assist financial institutions by promoting awareness and understanding of the risks and the mitigation activities associated with malware attacks in the financial industry, and identifying weaknesses in the ecosystem.

We therefore applaud any national initiative to alert citizens in situations where compromise of their systems is suspected, based on suspicious traffic detection methods discussed in the RFI. We fully support the objectives of this program

We provide the following answers to several of the questions posed in the RFI.

¹ BITS addresses issues at the intersection of financial services, technology and public policy, where industry cooperation serves the public good, such as critical infrastructure protection, fraud prevention, and the safety of financial services. BITS is the technology policy division of The Financial Services Roundtable, which represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Roundtable member companies provide fuel for America's economic engine, accounting directly for \$92.7 trillion in managed assets, \$1.2 trillion in revenue, and 2.3 million jobs. For more information, go to <http://www.bits.org/>.

A) Practices To Help Prevent and Mitigate Botnet Infections

(1) What existing practices are most effective in helping to identify and mitigate botnet infections? Where have these practices been effective? Please provide specific details as to why or why not.

Solutions such as those that the RFI envisions could inadvertently give citizens a false sense of security, feeling their provider (e.g., Internet service provider) will alert them to malware so they do not need to practice safe computing – avoid suspicious web sites, run anti-virus software, use strong passwords, etc. While defense in depth is an important measure, there is no substitute for safe end-user computing. Having said that, we do, however, see the provider alerts as a valuable supplement to a safe computing ecosystem.

(2) What preventative measures are most effective in stopping botnet infections before they happen? Where have these practices been effective? Please provide specific details as to why or why not.

There are a number of standard controls that may mitigate the risk, the first and most important is software change control. Software change control refers to a process whereby software is developed, compiled into packages for installation, labeled with version numbers, deployed by authorized personnel, and tracked on production systems. To be effective against malware, software change control processes must continue to track software through its deployment and operation. Changes to software must be automatically detected. Upon detection of a change, the change must be analyzed by someone with sufficient knowledge and reference materials to tell the difference between an authorized change and an unauthorized change. The reference materials should include tests such as cryptographic checksums that can be used to verify that code deployed in production is the same as the package that was delivered from a development environment or vendor. These detection processes must occur immediately after changes are detected. Changes must be detected on all operating system platforms and monitored for integrity, as malware operators are likely to attempt to disable or corrupt the software used for change monitoring.

Change monitoring should not be limited to software, but should extend to security configuration and role assignments such as start-up variables, firewall rules, and privileged accounts. Privileged account monitoring must be established in conjunction with a policy of authorized account usage so that authorized use may be distinguished from unauthorized use. For example, where users or software running in an administrator context is typical in a firm, this scenario used to install malware would not be detected as an intrusion. Even desktop administrators should be furnished with separate accounts reserved for privileged operations. Ideally, administrative access would be segmented so that systems would be subject to malware compromise via only a small percentage of total system users.

(4) Please identify existing practices that could be implemented more broadly to help prevent and mitigate botnet infections.

In addition to software change controls, control over the network periphery, vulnerability management, and log management are practices that can be used to prevent and mitigate botnet infections.

Control over the network periphery requires the establishment of a clear policy that allows administrators to determine authorized from unauthorized connections, and oversight that ensures compliance with these policies. Firewall rules and security configurations over all network equipment should also be subject to change control as described above for software. Organization's with network peripheries that are too large to manually review firewall rules in near real-time should have automated means to determine policy compliance for both inbound and outbound network connections. Lists of malicious sites are published and announced by various reliable sources. Connections to or from an organization to any published malicious site should be restricted via automated means. Both inbound and outbound network traffic should be examined for known malware patterns and signatures using intrusion and/or prevention detection systems. Any discretionary Internet traffic generated by an organizations users that may be a conduit for malicious content, such as email and web browsing, should be routed to choke points where proxy servers may be employed to inspect content for malware signatures as well as sensitive data. Proxy servers are frequently capable of decrypting encrypted web traffic, and these servers should block encrypted traffic if it cannot be decrypted for inspection (of course, exceptions may be made for authorized business applications).

Another key component of any malware mitigation strategy is vulnerability management. Operating system and application security standards should be established that, if followed, will ensure compliance with an organization's objectives for access to system programs, facilities, and data. These standards should be enforced with automated compliance-checking software, and that software should be monitored for integrity. All operating system and software security patches should be applied to any system for which they are available. Where vendors no longer support software patch processes, or do not commit to fixing security vulnerabilities in a given commercial product, organizations should consider alternative software vendors or versions for which security patches are available.

Organizations should also consider what may constitute evidence of malware intrusion in their technology environment, and identify patterns of activity that it may be possible to log and automatically detect in a manner that would trigger an incident response. Where it is not feasible to automate detection, manual log review procedures may be necessary to identify evidence of intrusion. Candidates for log monitoring include, but are not limited to, failed outbound email server connections attempts, network scanning, and excessive domain name queries. Due care should be exercised to ensure that the logs are collected as expected, and that they are archived with integrity.

Metrics on software change control, network periphery control, vulnerability management, and log management, as well as digital identity and incident response metrics, should be devised and employed as part of a comprehensive security management strategy. These metrics should be generated and reviewed as part of continuous operations monitoring processes and used in the course of daily security management.

(5) What existing mechanisms could be effective in sharing information about botnets that would help prevent, detect, and mitigate botnet infections?

The various sector Information Sharing and Analysis Centers, formed by sector members as a unique and specialized forum for managing risks to their organizations and infrastructure.

Members participate in national and homeland security efforts to strengthen infrastructure through cyber information sharing and analysis. As a result, members help their organizations improve their incident response through trusted collaboration, analysis, coordination, and drive decision-making by policy makers on cybersecurity, incident response, and information sharing issues.

(7) Upon discovering that a consumer's computer or device is likely infected by a botnet, should an ISP or other private entity be encouraged to contact the consumer to offer online support services for the prevention and mitigation of botnets? If so, how could support services be made available? If not, why not?

Yes. ISPs that detect malware should warn or educate the system owner, and/or quarantine the affected system as appropriate to safeguard other systems.

B. Effective Practices for Identifying Botnets

(12) To date, many efforts have focused on the role of ISPs in detecting and notifying consumers about botnets. It has been suggested that other entities beyond ISPs (such as operating system vendors, search engines, security software vendors, etc.) can participate in anti-botnet related efforts. Should voluntary efforts focus only on ISPs? If not, why not? If so, why and who else should participate in this role?

No. The list below identifies several stakeholders who could be partnering with their customers to improve the cyber ecosystem's overall resistance to malware.

Advertising Services - A wide variety of media outlets sell advertising to media, retail, and other internet sites. These services should provide due diligence to ensure that malware is not delivered via advertisements.

Anti-Malware Vendors - Anti-Malware software vendors should improve malware detection capability by pursuing advances in both methods and timing for client updates. They should participate in efforts to establish malware detection metrics.

Anti-Malware software vendors should also improve malware isolation features, fail in safe mode, and also ship products with the more secure settings as default.

Application Stores - Application Stores vend software for a variety of digital devices, including mobile phones and desktops. They should improve due diligence efforts to ensure the applications they sell do not contain known malware or otherwise obviously suspect software.

Certificate Authorities - Certificate Authorities (CA) play a key role in the security of online banking applications in that proper application of the technology allows a customer to identify imitation banking sites. However, recent failure in the security of CA administrative functions secure has resulted in issuance of "valid" SSL and EV-SSL certifications to criminal elements. CA need to evolve their technology and service offerings to prevent these malicious activities.

Domain Name Service Registrars - Domain Name Service (DNS) Registrars should play a key role in malware prevention by improving due diligence so that cybercriminals find it harder to register new domains to perpetrate phishing attacks and/or malware drive-by sites.

It is absolutely critical that DNS Registrars maintain accurate data on domain name owners so organizations can perform effective investigation into instances of abuse. Unavailable or inaccurate registration data increases the cost of online fraud investigation and remediation activity.

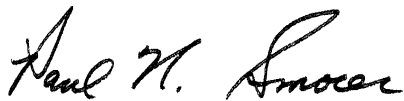
Email Hosts - Various industry standards have been developed to prevent email spoofing and spamming at the server level. Email hosts should observe Internet Engineering Task Force standards and BITS recommendations for enabling email authentication and validation processing on both inbound and outbound mail streams.

ICANN - ICANN issues generic Top Level Domains (gTLDs) for specific purposes but generally does not enforce the manner in which they are used (e.g. .com, .edu). As an example, a gTLD issued for financial services should be restricted to FI registrations. In this environment, technologies could automatically provide higher levels of security for FI online services.

Mail User Agent Vendors - Mail User Agents like Outlook, Apple Mail, Thunderbird, etc. can help prevent malware infections by leveraging security indicators and business rules that users can leverage to identify when a message in their inbox (or spam folder) is suspect.

If you have any questions or comments, please feel free to contact me at 202-589-2437 or PaulS@fsround.org or William Henley, BITS Senior Vice President for Regulation, at 202-589-2402 or William@fsround.org.

Sincerely,

A handwritten signature in black ink that reads "Paul M. Smocer". The signature is written in a cursive, flowing style.

Paul Smocer
President