Response of FireEye to DOC and NIST RFI on Developing a Framework to Improve Critical Infrastructure Security

FireEye appreciates the opportunity to provide comments to the Department of Commerce and National Institute of Standards and Technology's Request for Information on Developing a Framework to Improve Critical Infrastructure Cybersecurity ("Framework"). This is a critical step that will enable the essential shift from reactive to proactive cyber defense and enhance the cyber posture of critical infrastructure in the United States.

- FireEye's recommends that the standards, guidelines, frameworks and best practices prioritized in **the Framework emphasize mitigation measures designed to combat advanced cyber threats targeting unknown vulnerabilities.**

    - Critical infrastructure companies are under constant attack, targeted by increasingly sophisticated and well-funded criminals and nation-states seeking to steal, compromise, alter, or destroy sensitive information. The rapid evolution of malware is essentially a cyber "arms race" run by organizations with geopolitical agendas and profit motives.

    - Never seen before "zero-day" attacks target undocumented vulnerabilities and polymorphic techniques allow malware to easily bypass traditional, signature based defenses including antivirus, network firewalls and intrusion prevention systems.

        - Sophisticated attackers can combine Web, email, and file-based attack vectors in a staged and blended attack, making it far more likely for their attacks to go undetected.
        - Many attackers penetrate systems by hiding newly minted polymorphic malware on innocent Web pages and embedded in downloadable files like JPEG pictures and PDF documents.
        - Or they use personalized, "spear" phishing emails sent to carefully selected victims with a plausible-looking message and a malicious attachment or a URL to a malicious site.

    - With the dramatic proliferation of sophisticated malware available in the wild, advanced techniques that were once entirely the domain of well-funded nation-states are now in the hands of terrorist groups and rogue states, or anyone with a credit card and $200.00.

- Based on FireEye's research, organizations are experiencing explosive growth in these kinds of attacks. On average, organizations are experiencing 221 web-based malicious events per week that successfully evade traditional defenses. Compared to the second half of 2011, the number of events per organization rose by 225% in the first half of 2012. Malware is so prevalent that, on average, enterprises experience a malware-related event once every three minutes.

- FireEye recommends that the Framework include a section **on standards and best practices that counter advanced adversary tactics and techniques** such as targeted spear phish, zero-day and blended attacks. This section should emphasize automated, proactive and dynamic defense by incorporating the following as baseline standards and best practices:

  - **Signature-less, proactive defense that detects and blocks unknown cyber-attacks over the lifecycle of an attack** as a necessary complement to traditional, signature based defenses such as firewalls, intrusion prevention systems, web and email gateways and anti-virus software. Recommended attributes of such tools include the ability to:

    - Identify and block in-bound zero day attacks across multiple threat vectors;
    - Expose the entire attack life cycle by correlating intelligence across various threat vectors;
    - Block outreach from a compromised host to its command and control center;
    - Prevent the exfiltration of data and the download of additional malware;
    - Eliminate false positives; and
    - Produce complete forensic details.

  - Tools that provide **automated sharing of indicators of compromise in near real time** at the local, enterprise and global levels.

  - **Virtualization techniques for the identification of known and unknown malware** as described in **Security Control 44, Detonation Chambers, which was recently added to NIST Special Publication 800.53, Revision 4 (Final Public Draft) Recommended Security Controls for Federal Information Systems and Organizations.** The Supplemental Guidance to Security Control 44 provides:

Detonation chambers, also known as dynamic execution environments, allow organizations to open email attachments, execute untrusted applications, and/or execute Universal Resource Locator (URL) requests in the safety of an isolated environment. These protected and isolated execution environments provide a means of determining whether the associated attachments/applications contain malware. While related to the concept of deception nets, the control is not intended to maintain a long-term environment in which adversaries can operate and their actions can be observed. Rather, it is intended to quickly identify malware and reduce the likelihood of malware spreading to user environments of operation.

- FireEye further recommends that the Framework embrace innovation and encourage the rapid adoption of new capabilities by critical infrastructure companies and government initiatives that enhance protections for critical infrastructure. To further these imperatives, FireEye recommends that the Framework be updated frequently to incorporate new and innovative capabilities that mitigate risk from emerging threats.