Enhancing Resilience of the Internet and Communications Ecosystem

NIST National Cybersecurity Center of Excellence, Rockville MD

July 11-12, 2017

Workshop Purpose: The purpose of this workshop is to explore a range of current and emerging solutions to enhance the resilience of the Internet against automated distributed threats, such as botnets. Deployment of these solutions will depend upon the ability and willingness of various parties to take action. Depending upon the specific solution, actions may be required by infrastructure providers, device manufacturers, system and network owners, research community, government, and/or standards developers. By exploring the solution space with a broad cross-section of participants, NIST hopes to identify promising avenues for all parties to enhance the resilience of the Internet.

Workshop Output: NIST will produce a workshop proceedings document that summarizes the session discussions, captures findings, and identifies opportunities for next steps. Outputs of this workshop will also serve as input to implementation activities related to Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Agenda

Tuesday July 11, 2017

7:30	**Registrant Check-In**
8:30	**Welcome and Workshop Overview**
8:45	**Setting the Stage** *This plenary session will summarize the problem space (e.g., the botnet ecosystem), identify stakeholders (standards/protocol developers, infrastructure providers, consumers, manufacturers, regulators) in botnet mitigation, and review past approaches and outputs.* **Ari Schwartz, Venable**
9:30	**Infrastructure Provider's Perspective: Current and Emerging Standards, Best Practices, and Technologies (Panel 1)** *This plenary session will explore current efforts and future opportunities to enhance the resilience of the infrastructure (e.g., the Internet). This panel will discuss current state, trends, and current and promising approaches to mitigate automated distributed threats such as DDOS, with particular focus on botnets and IoT.* **Russ Housley, Vigilsec (moderator)** **Richard Barnes, Cisco** **Arabella Hallawell, Arbor Networks** **Danny McPherson, VeriSign** **Brian Rexroad, AT&T**

10:15	**Break**
10:30	**Session 1 Breakout (assigned)**
12:00	**Lunch**
1:00	**Product Development (Panel 2)** *This plenary session will explore current efforts and future opportunities for network component and device manufacturers (including IoT solution providers) to address the root causes of recent botnets (unconstrained network access, hard coded passwords, and buggy software). Session scope includes both enterprise and home use.* **Yolonda Smith, Pwnie Express (moderator)** **Anura S. Fernando, Underwriters Laboratory** **Jeff Greene, Symantec** **Rob Spiger, Microsoft** **Eric Wenger, Cisco**
1:45	**Session 2 Breakout (assigned)**
3:00	**Break**
3:15	**Customer Perspective: Current Approaches (Panel 3)** *This plenary session will explore how Internet users, particularly in the enterprise, can protect themselves, and avoid being part of the problem. Panelists will begin with an overview of the challenges an enterprise might face from distributed attacks, including DDoS, web applications, and fraud. Discussion will highlight the capabilities and limitations of best current practices and emerging technologies, and the potential for cross-sector collaboration.* **Nadya Bartol, Boston Consulting Group (moderator)** **Steve Curren, HHS Office of the Assistant Secretary for Preparedness and Response** **Matt Eggers, US Chamber of Commerce** **Bradley Nix, Deputy Director for US-CERT at the NCCIC, DHS** **Spencer Wilcox, Exelon**
4:00	**Session 3 Breakout (assigned)**
5:00	**Adjourn Day 1**

July 12, 2017

7:30	**Registrant Check-In**
8:30	**Welcome and Opening Remarks**
8:45	**Research Directions** *This panel will identify and explore gap areas in approaches to mitigating botnets, and highlight opportunities to address those gaps.* **Pat Muoio, Cybertech Consulting (moderator)** **David Dagon, Ga Tech** **Keith Marzullo, Univ. of MD** **Phil Reitinger, Global Cyber Alliance**
9:30	**The Government Role** *This plenary session will discuss current efforts and future opportunities for governments to enhance the resilience of the infrastructure, which may include policy and regulatory approaches, incentives and market motivators, economic impacts, and international considerations.* **Grace Koh, NEC (moderator)** **Andi Arias, FTC** **Tom Grasso, FBI** **John Nicholson, UK Embassy** **Malikah (Mikki) Smith, HHS/ONC**
10:15	**Break**
10:30	**Research & Government Role Breakouts**
11:15	**Break**
11:30	**Summary of Day 1 Breakout Sessions**
12:00	**Open Discussion**
12:30	**Closing and Next Steps (DOC/DHS)**
12:45	**Adjourn**