CSRIC III
Communications Security, Reliability and Interoperability Council

Working Group 7: Botnet Remediation

March 22, 2012

Michael O'Reirdan (MAAWG) - Chair
Peter Fonash (DHS) – Vice-Chair

WG 7 Objectives

Working Group 7 – Botnet Remediation

Description: This Working Group will review the efforts undertaken within the international community, such as the Australian Internet Industry Code of Practice, and among domestic stakeholder groups, such as IETF and the Messaging Anti-Abuse Working Group, for applicability to U.S. ISPs. Building on the work of CSRIC II Working Group 8 ISP Network Protection Practices, the Botnet Remediation Working Group shall propose a set of agreed-upon voluntary practices that would constitute the framework for an opt-in implementation model for ISPs. The Working Group will propose a method for ISPs to express their intent to op-into the framework proposed by the Working Group.

The Working Group will also identify potential ISP implementation obstacles to the newly drafted Botnet Remediation business practices and identify steps the FCC can take that may help overcome these obstacles.

Finally, the Working Group shall identify performance metrics to evaluate the effectiveness of the ISP Botnet Remediation Business Practices at curbing the spread of botnet infections.

CSRIC III
Communications Security, Reliability and Interoperability Council

WG 7 Members

Name	Organization
Michael O'Reirdan (Chair)	MAAWG
Peter Fonash (Vice Chair)	DHS
Robert Thornberry (Editor)	Alcatel-Lucent
Alex Bobotek	AT&T
John Denning	Bank of Amer.
Neil Schwartzman (Secretary)	CAUCE
Michael Glenn	CenturyLink
Paul Diamond (Editor)	CenturyLink
Jay Opperman	Comcast
Matt Carothers	Cox
Gunter Ollmann	Damballa

Name	Organization
Brian Done	DHS
Daniel Bright	EMC Inc
Kurian Jacob	FCC
Vern Mosley	FCC
Bill McInnis	IID
Chris Sills	IID
Tim Rohrbaugh	Intersections
Barry Greene	ISC
Merike Kaeo	ISC
Kevin Sullivan	Microsoft
Jon Boyens	NIST
Craig Spiezle	OTA
Bill Smith	PayPal
Gabe Iovino	REN-ISAC
Johannes Ullrich	SANS Institute

Name	Organization
Adam O'Donnell	Sourcefire
Alfred Huger	Sourcefire
Greg Holzapfel	Sprint
James Holgerson	Sprint
Michael Fiumano	Sprint
Maxim Weinstein	StopBadware
Tice Morgan	T-Mobile
John Griffin	TCS
Chris Roosenraad	TWC
Joe St Sauver (Glossary)	Univ of Oregon/ Internet 2
Robert Mayer	USTelecom Assoc.
Eric Osterweil	Verisign
John St. Clair	Verizon
Timothy Vogel	Verizon

CSRIC III
Communications Security, Reliability and Interoperability Council

Work Plan

Phase 1: Based on CSRIC II output, MAAWG recommendations and IETF draft, produce initial Code of Conduct

- March 2012

Phase 2: Identify Barriers to Code Participation

- September 2012

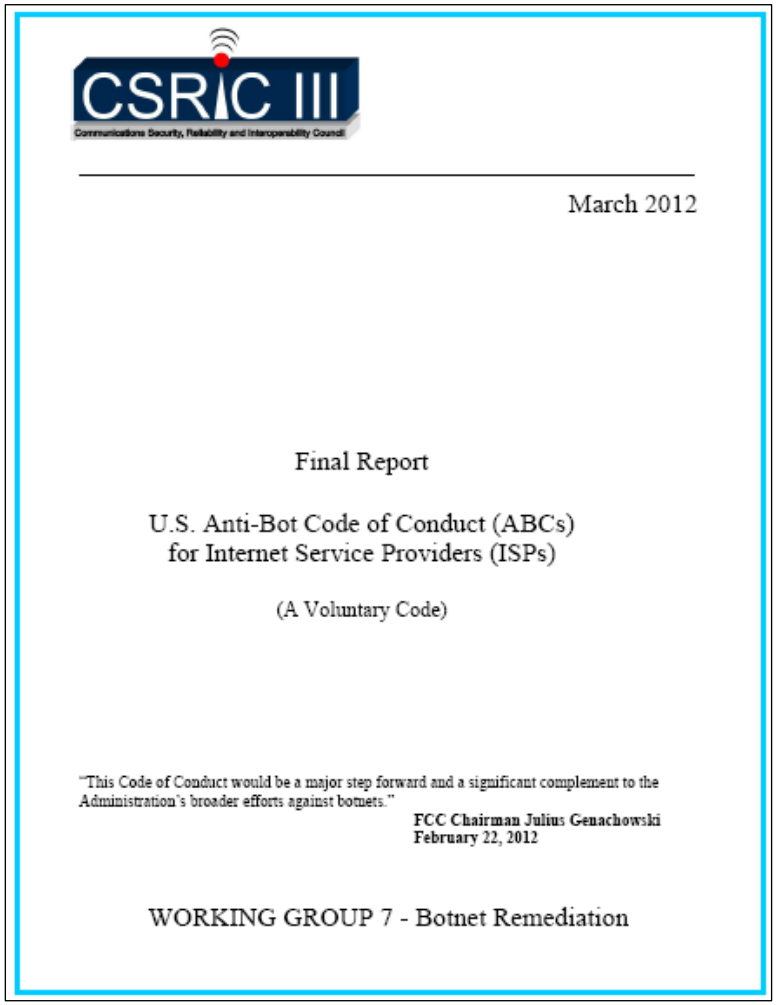
Phase 3: Develop Bot Metrics

- December 2012

CSRIC III
Communications Security, Reliability and Interoperability Council

Status

✓Phase 1: U.S. Anti-Bot Code of Conduct (ABCs) for Internet Service Providers (ISPs) completed



CSRIC III
Communications Security, Reliability and Interoperability Council

March 2012

Final Report

U.S. Anti-Bot Code of Conduct (ABCs)
for Internet Service Providers (ISPs)

(A Voluntary Code)

"This Code of Conduct would be a major step forward and a significant complement to the Administration's broader efforts against botnets."

FCC Chairman Julius Genachowski
February 22, 2012

WORKING GROUP 7 - Botnet Remediation

CSRIC III
Communications Security, Reliability and Interoperability Council

U.S. Anti-Bot Code of Conduct

- Voluntary U.S. Code provides an initial framework for ISPs to better understand and help address the bot issue
- Objective of Code is to encourage ISPs to participate in each of the following activities:
  - end-user education to prevent bot infections,
  - detection of bots,
  - notification of potential bot infections,
  - remediation of bots, and
  - collaboration and sharing of information.

CSRIC III
Communications Security, Reliability and Interoperability Council

U.S. Anti-Bot Code of Conduct (cont.)

- Implementation of the Code guided by the following principles:
  - Voluntary – encourages voluntary types of actions to be taken by ISPs
  - Technology Neutral – does not prescribe particular means or methods
  - Approach Neutral – does not prescribe any particular approach
  - Respect for Privacy – address privacy issues in accordance with laws
  - Legal Compliance – address other areas in accordance with laws
  - Shared Responsibility – other Internet ecosystem participation needed
  - Sustainability – ISP activities should be cost-effective and sustainable
  - Information Sharing – ISPs share lessons-learned with other stakeholders
  - Effectiveness – encourages ISP activities that are appropriate and effective
  - Effective Communication – ISP communication with customers easily understood and accessible by the recipients

CSRIC III
Communications Security, Reliability and Interoperability Council

WG7 Recommendations

- Working Group 7 recommends actions that ISPs offering residential broadband Internet access may take if they choose to adopt the Code

- Working Group 7 further recommends ISPs and other service providers indicate their agreement to participate in the voluntary Code by contacting the entity of their choice, or self-asserting on their company webpage

CSRIC III
Communications Security, Reliability and Interoperability Council

Next Steps

- Determine long-term administration of Code participation
- Begin Phase 2 - Identification of Barriers to Code Participation
- Phase 3 – Develop bot Metrics - started

CSRIC III
Communications Security, Reliability and Interoperability Council