



# **Working Group 5: Remediation of Server-Based DDoS Attacks**

## **Status Update**

December 4, 2013

Peter Fonash (DHS), Co-Chair

Michael Glenn (CenturyLink), Co-Chair

# WG5 Objectives

## Description:

Critical infrastructure sectors, including the financial sector, have been under assault from a barrage of DDoS attacks emanating from data centers and hosting providers. **This Working Group will examine and make recommendations to the Council regarding network level best practices and other measures to mitigate the effects of DDoS attacks from large data centers and hosting sites.** These recommendations should include technical and operational methods and procedures to facilitate stakeholder implementation of the recommended solution(s).

## Deliverable:

Recommended measures communications providers can take to mitigate the incidence and impact of DDoS attacks from data centers and hosting providers, particularly those targeting the information systems of critical sectors.



# WG5 Members

- WG5 has assembled a team of 47 members, including representatives from ISPs, banks, hosting providers, non-profits, associations, academia, federal and state governments, and security experts to accomplish the CSRIC IV charge

Name	Organization	Name	Organization	Name	Organization
Peter Fonash (Co-Chair)	DHS	Dale Drew	Level 3	Eric Osterweil	VeriSign, Inc.
Mike Glenn (Co-Chair)	CenturyLink	David Fernandez	Prolexic Technologies	Wayne Pacine	Fed Reserve Board of Governors
Paul Diamond (Co-Editor)	CenturyLink	Michael Geller	ATIS	Glen Pirrotta	Comcast
Bob Thornberry (Co-Editor)	Bell Labs, Alcatel-Lucent	Mark Ghassemzadeh	ACS	R.H. Powell	Akamai
Vern Mosley (FCC Liaison)	FCC	Darren Grabowski	NTT	Nick Rascona	Sprint
Jared Allison	Verizon	Sam Grosby	US Bank	Jim Reavis	Cloud Security Alliance
Don Blumenthal	Public Interest Registry	Dave LaBianca	FS-ISAC	Chris Roosenraad	Time Warner Cable
Chris Boyer	AT&T	Alan Langford	Joomla	Craig Spiezle	Online Trust Alliance
Matt Bretan	Goldman Sachs	John Levine	CAUCE	David Stoline	Drupal
Matt Carothers	Cox Communications	Greg Lucak	Windstream	Joe St Sauver	Univ of Oregon/Internet2
Roy Cormier	Nsight	John Marinho	CTIA	Kevin Sullivan	Microsoft
Kyle Davis	Department of Treasury	Dan Massey	IEEE	Bernie Thomas	CSG International
Dave DeCoster	Shadowserver	Ron Mathis	Intrado	Jason Trizna	Amazon Web Services
John Denning	Bank of America	Bill McInnis	Internet Identity	Errol Weiss	FSSCC
Roland Dobbins	Arbor Networks	Chris Morrow	Google	Pam Witmer	PA PUC
Martin Dolly	ATIS	Mike O'Reirdan	MAAWG		



# Background

- CSRIC II

- in December 2010, approved WG8's recommendations from their final report *ISP Network Protection Practices*

- recommended BPs in areas of prevention, detection, notification, mitigation, and privacy considerations
    - focused on best practices (BPs) for ISPs that provide services to consumers on residential broadband networks, but noted many of the best practices identified in the report would also be valuable practices to apply in non-consumer, non-residential network contexts
    - further recommended that, at a later date, the FCC consider whether additional best practice work would be valuable in the non-residential context



# Background (cont.)

- CSRIC III

- in March 2013, approved WG7's recommendations from their final report *U.S. Anti-Bot Code of Conduct for ISPs (ABCs for ISPs)*

- focused on botnet threat from residential broadband clients
    - recommended voluntary ISP actions in areas of education, detection, notification, remediation, and collaboration
    - further recommended the FCC, working in partnership with other federal government agencies and industry, facilitate the creation of case studies on bot mitigation activities



# Background (cont.)

- CSRIC III

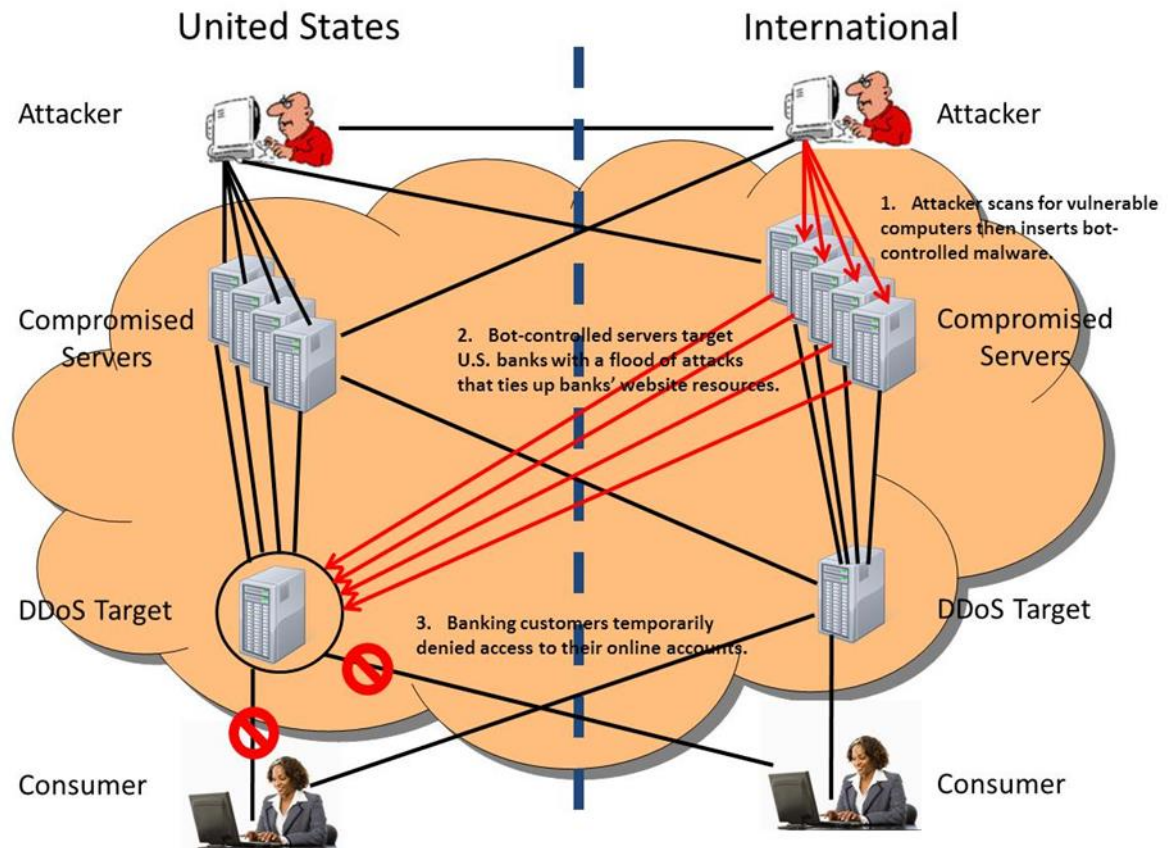
- in September 2012 and March 2013, approved WG4's recommendations from their final reports, *BGP Security Best Practices and DNS Best Practices*

- provided recommendations to mitigate or remediate BGP interface, resource, and internal bandwidth exhaustion denial of service attacks
    - provided recommendations to mitigate or remediate direct DNS recursive and authoritative denial of service attacks.
    - provided recommendations for minimizing reflective DNS denial of service attacks.



# Background (cont.)

- Recent DDoS attacks have exploited vulnerabilities in web-hosting companies and other large data centers to launch DDoS attacks on computer systems and websites



An Illustrative Example

# Background (cont.)

- CSRIC IV WG5 efforts will leverage and complement other botnet activities, including:
  - CSRIC III WG4 DDoS Mitigation Recommendations
  - Messaging, Malware, Mobile Anti-Abuse Working Group (M<sup>3</sup>AAWG)
  - Online Trust Alliance (OTA) Anti-Botnet Working Group
  - Cloud Security Alliance (CSA)
  - Industry Botnet Group (IBG)





# WG5 Approach

- Identify WG5 subgroups: ISPs, Financial Community, Internet Security Experts, and Best Practices Review
- The ISPs, Financial Community, and Internet Security Experts subgroups will develop representative case studies for server-based DDoS attacks
  - For each case study, subgroups identify network level actions taken to:
    - Identify, Protect, Detect, Respond, and Recover from the attacks
- Best Practices Review subgroup identifies applicable BPs
  - Using case studies, WG5 determines if best practices were followed, or if gaps exist, in each of the representative case studies
- Whole WG5 then integrates subgroups' work and documents or develops network level best practices and other measures to mitigate the effects of DDoS attacks from large data centers and hosting sites



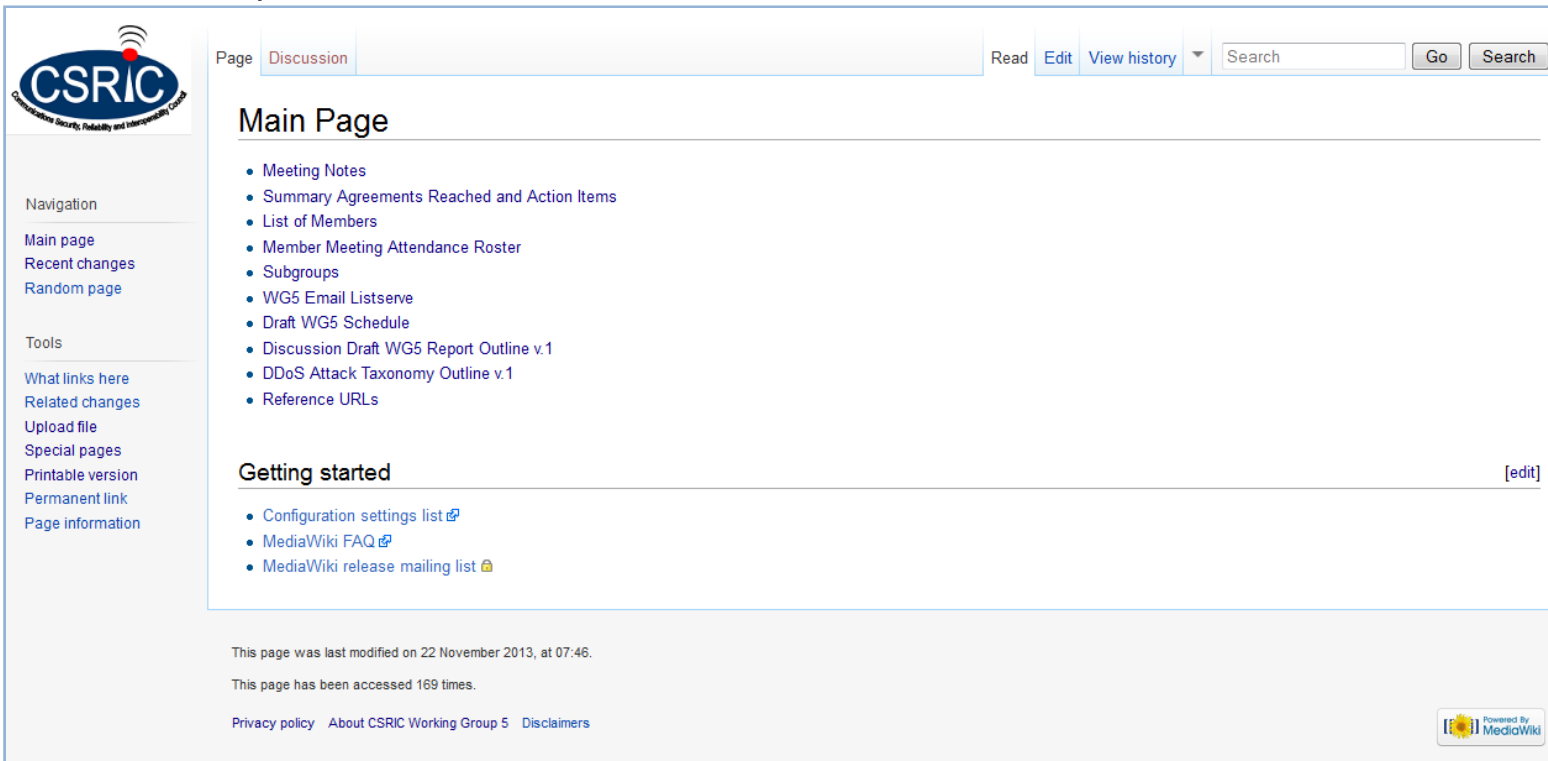
# WG5 Status

- WG5 has held five biweekly conference calls with its working group members to discuss the CSRIC IV charge, develop an approach and schedule to accomplish the tasking, and segment the work amongst subgroups according to subject matter expertise
- WG5 subgroup leads have been identified and have begun biweekly conference calls as well



# WG5 Wiki

- In order to facilitate information sharing amongst WG5 members, a WG5 wiki was created



The screenshot shows the main page of the WG5 Wiki. At the top left is the CSRIC logo (Communications Security, Reliability and Interoperability Council). The page title is "Main Page". Below the title is a list of links: Meeting Notes, Summary Agreements Reached and Action Items, List of Members, Member Meeting Attendance Roster, Subgroups, WG5 Email Listserve, Draft WG5 Schedule, Discussion Draft WG5 Report Outline v.1, DDoS Attack Taxonomy Outline v.1, and Reference URLs. Below this is a "Getting started" section with links to Configuration settings list, MediaWiki FAQ, and MediaWiki release mailing list. The page footer includes the text "This page was last modified on 22 November 2013, at 07:46." and "This page has been accessed 169 times." There are also links for Privacy policy, About CSRIC Working Group 5, and Disclaimers. A "Powered by MediaWiki" logo is in the bottom right corner.

Page [Discussion](#) [Read](#) [Edit](#) [View history](#)

## Main Page


- [Meeting Notes](#)
- [Summary Agreements Reached and Action Items](#)
- [List of Members](#)
- [Member Meeting Attendance Roster](#)
- [Subgroups](#)
- [WG5 Email Listserve](#)
- [Draft WG5 Schedule](#)
- [Discussion Draft WG5 Report Outline v.1](#)
- [DDoS Attack Taxonomy Outline v.1](#)
- [Reference URLs](#)

### Getting started [\[edit\]](#)

- [Configuration settings list](#)
- [MediaWiki FAQ](#)
- [MediaWiki release mailing list](#)

This page was last modified on 22 November 2013, at 07:46.  
This page has been accessed 169 times.

[Privacy policy](#) [About CSRIC Working Group 5](#) [Disclaimers](#)

Powered by  MediaWiki



# WG5 Schedule

- Bi-weekly conference calls with all WG5 members
- Subgroups hold bi-weekly conference calls on opposite weeks
- Quarterly face-to-face meetings (with phone-in option for those unable to travel)
  - January 8<sup>th</sup> & 9<sup>th</sup> - scheduled
  - April and August - tentative
- June 2014 – Draft Final WG5 Report
- September 2014 – Final WG5 Report



# Next Steps

- Develop common case-study template for subgroups to use
- Develop DDoS Attack Taxonomy
- Document case-studies using above template and taxonomy
- Review existing Best Practices for applicability to server-based DDoS attacks
- Integrate subgroups' work into recommended Best Practices
- Continue bi-weekly conference calls
- Provide periodic status updates to Steering Committee and Council

