CSRIC
Communications Security, Reliability and Interoperability Council

Working Group 5: Remediation of Server-Based DDoS Attacks

Status Update

March 20, 2014

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 48 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	Wells Fargo	Jim Reavis	Cloud Security Alliance
Don Blumenthal	Public Interest Registry	Rodney Joffe	Neustar	Chris Roosenraad	Time Warner Cable
Chris Boyer	AT&T	Dave LaBianca	FS-ISAC	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	Matt Tooley	NCTA
John Denning	Bank of America	Bill McInnis	Internet Identity	Jason Trizna	Amazon Web Services
Roland Dobbins	Arbor Networks	Chris Morrow	Google	Errol Weiss	FSSCC
Martin Dolly	ATIS	Mike O'Reirdan	MAAWG	Pam Witmer	PA PUC

WG5 Approach

- Identify WG5 subgroups: ISPs, Financial Community, Internet Security Experts, and Best Practices Review
  - Best Practices Review subgroup identifies applicable BPs for DDoS server-based attacks
  - The ISPs, Financial Community, and Internet Security Experts subgroups develop representative case studies for server-based DDoS attacks
    - 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 biweekly conference calls with its working group members to accomplish the tasking
- Subgroups have held biweekly conference calls to solicit input and review their case study deliverables
- WG5 held a two-day face-to-face meeting in January to facilitate discussion among, and receive initial readouts, from the subgroups
- WG5 subgroups in final stages of preparing case study deliverables for review by all WG5 members

CSRIC
Communications Security, Reliability and Interoperability Council

Best Practice Review Subgroup

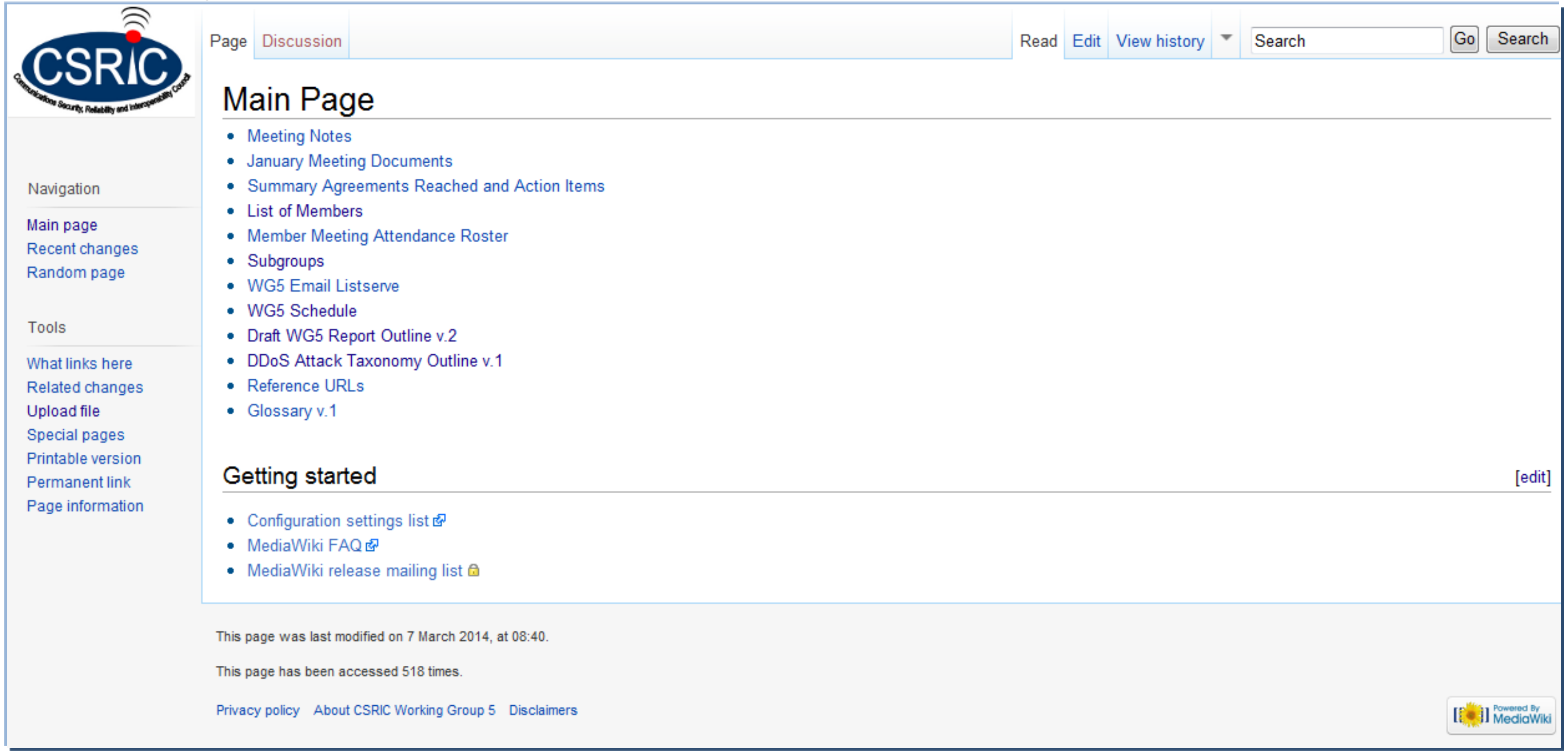
- Reviewed approximately 600 cybersecurity BPs to determine whether or not they were within scope of WG5 tasking (i.e., BPs to mitigate server-based DDoS attacks)
- Initial review suggests approximately 10% - 15% of BPs reviewed are within scope of WG5 tasking
- Subset of BPs determined to be within scope provided to other subgroups for their use in analysis of case studies

ISP, Financial, and Internet Security Experts Subgroup Status

- Actions underway to:
  - Confirm the In-Scope/Out-of-Scope determination made by the Best Practices subgroup
  - Determine which Best Practices apply to their case studies
  - Identify gaps
  - Propose new Best Practices to address gaps

WG5 Wiki

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



Main Page

- Meeting Notes
- January Meeting Documents
- Summary Agreements Reached and Action Items
- List of Members
- Member Meeting Attendance Roster
- Subgroups
- WG5 Email Listserve
- WG5 Schedule
- Draft WG5 Report Outline v.2
- DDoS Attack Taxonomy Outline v.1
- Reference URLs
- Glossary v.1

Getting started

- Configuration settings list
- MediaWiki FAQ
- MediaWiki release mailing list

This page was last modified on 7 March 2014, at 08:40.

This page has been accessed 518 times.

WG5 Schedule

- Bi-weekly conference calls with all WG5 members
- Quarterly face-to-face meetings (with phone-in option for those unable to travel)
  - ✓ January 8th & 9th
  - – April 9th & 10th – scheduled
  - – August - tentative
- June 18, 2014 – Draft Interim WG5 Report
  - –Detailed plan developed – seen as an aggressive schedule
- September 30, 2014 – Final WG5 Report

Next Steps

- Finalize review of initial subset of Best Practices for applicability to server-based DDoS attacks
- Subgroups finalize case studies
- Integrate subgroups' work into recommended Best Practices
- Begin preparation of draft interim report
- Continue bi-weekly conference calls
- Hold second face-to-face meeting in preparation for draft interim report
- Provide periodic status updates to Steering Committee and Council

CSRIC
Communications Security, Reliability and Interoperability Council