Working Group 5: Remediation of Server-Based DDoS Attacks

Status Update

September 12, 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

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

Background

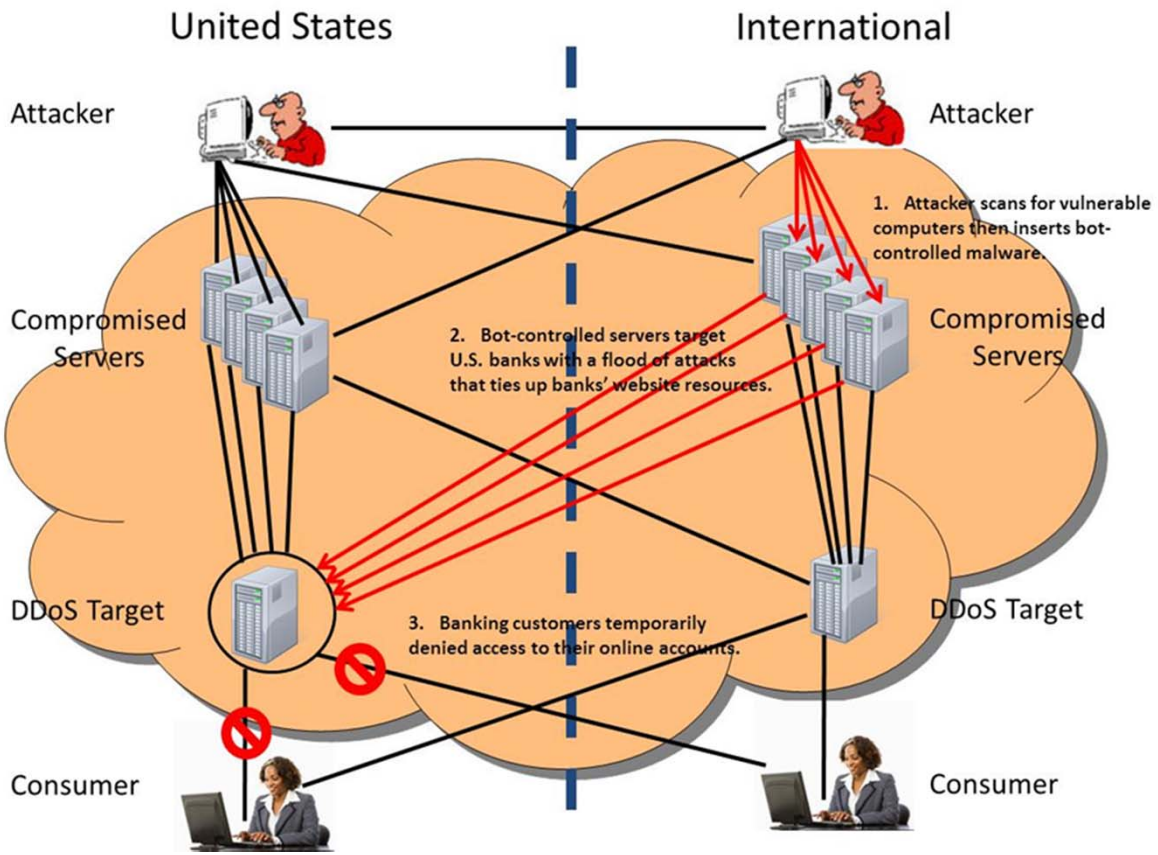
- CSRIC II
  - in December 2010, approved WG8's recommendations from their final report *ISP Network Protection Practices*
    - recommended BPs in areas of prevention, detection, notification, mitigation, and privacy considerations
    - focused on best practices (BPs) for ISPs that provide services 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.)

- 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 WG5 efforts will complement other botnet activities, including:
  - Online Trust Alliance (OTA) Anti-Botnet Working Group[1]
    - multi-stakeholder focus to develop and promote best practices to help prevent, detect, remediate, and recover from the threat of bots and related malicious activities
  - Cloud Security Alliance (CSA)[2]
    - cloud security stakeholder focus to develop and promote best practices
  - Industry Botnet Group (IBG)[3]
    - web host focus to develop best practices to mitigate effects of data center botnets

[1] https://otalliance.org/botnets.html

[2] https://cloudsecurityalliance.org

[3] http://www.industrybotnetgroup.org

WG5 Status

• CSRIC IV WG5 charged to 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

• WG5 has assembled a team of 40 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

WG5 Status (cont.)

- WG5 held a kickoff conference call with its working group members to discuss the CSRIC IV charge, develop an approach to accomplish the tasking, and develop the status update to the Council

WG5 Approach

- Develop representative case studies for server-based DDoS attacks
- For each case study, identify network level actions taken to:
  - Prevent, Deter, Detect, Notify, Defend, Remediate, and Recover from the attacks
- Determine if best practices were followed, or if gaps exist, in each of the above areas
- Document or develop network level best practices and other measures to mitigate the effects of DDoS attacks from large data centers and hosting sites

WG5 Schedule

- Bi-weekly conference calls with members
- Quarterly face-to-face meetings (with phone-in option for those unable to travel)
- June 2014 – Draft Final WG5 Report
- September 2014 – Final WG5 Report

Next Steps

- Firm up WG5 membership
- Revise initial work plan, based on member input, to accomplish the CSRIC IV charge
- Seek WG5 volunteers to lead development of case studies
- Schedule first face-to-face meeting
- Continue bi-weekly conference calls
- Provide periodic status updates to Steering Committee and Council