Working Group 5: Remediation of Server-Based DDoS Attacks

Status Update

June 18, 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 41 members, including representatives from ISPs, financial institutions, hosting providers, non-profits, associations, academia, federal and state governments, and security experts to accomplish the CSRIC IV charge

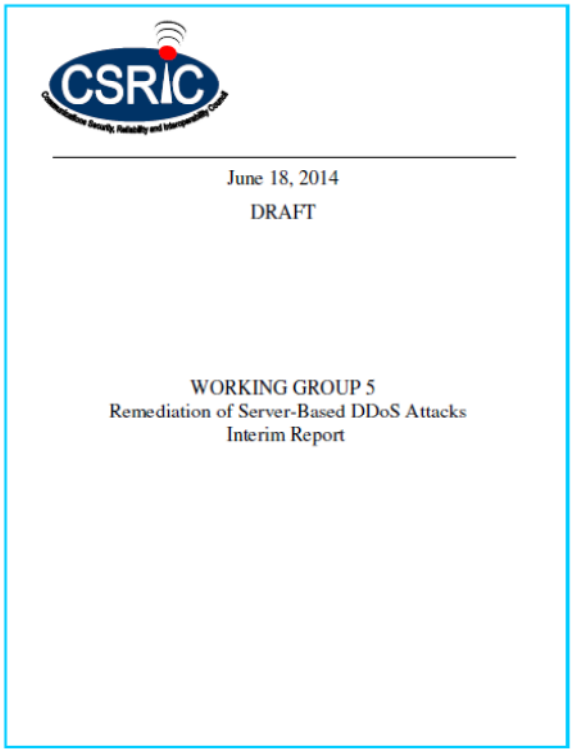
Name	Organization	Name	Organization	Name	Organization
Peter Fonash (Co-Chair)	DHS	David Fernandez	Prolexic Technologies	Wayne Pacine	Fed Reserve Board of Governors
Mike Glenn (Co-Chair)	CenturyLink	Mark Ghassemzadeh	ACS	Glen Pirrotta	Comcast
Paul Diamond (Co-Editor)	CenturyLink	Darren Grabowski	NTT	R.H.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

WG5 Status

- WG5 held a 2-day face-to-face meeting in April, hosted by Intrado (Longmont, CO)
  - reviewed draft server-based DDoS attack remediation best practices, identified gaps in best practices, and began drafting text of Interim Report
- WG5 delivered its Interim Report June 13th
  - Comments on report requested NLT July 11th
- Comments received will be factored into Final Report, due in September 2014

Interim Report

Table of Contents



June 18, 2014

DRAFT

WORKING GROUP 5
Remediation of Server-Based DDoS Attacks
Interim Report

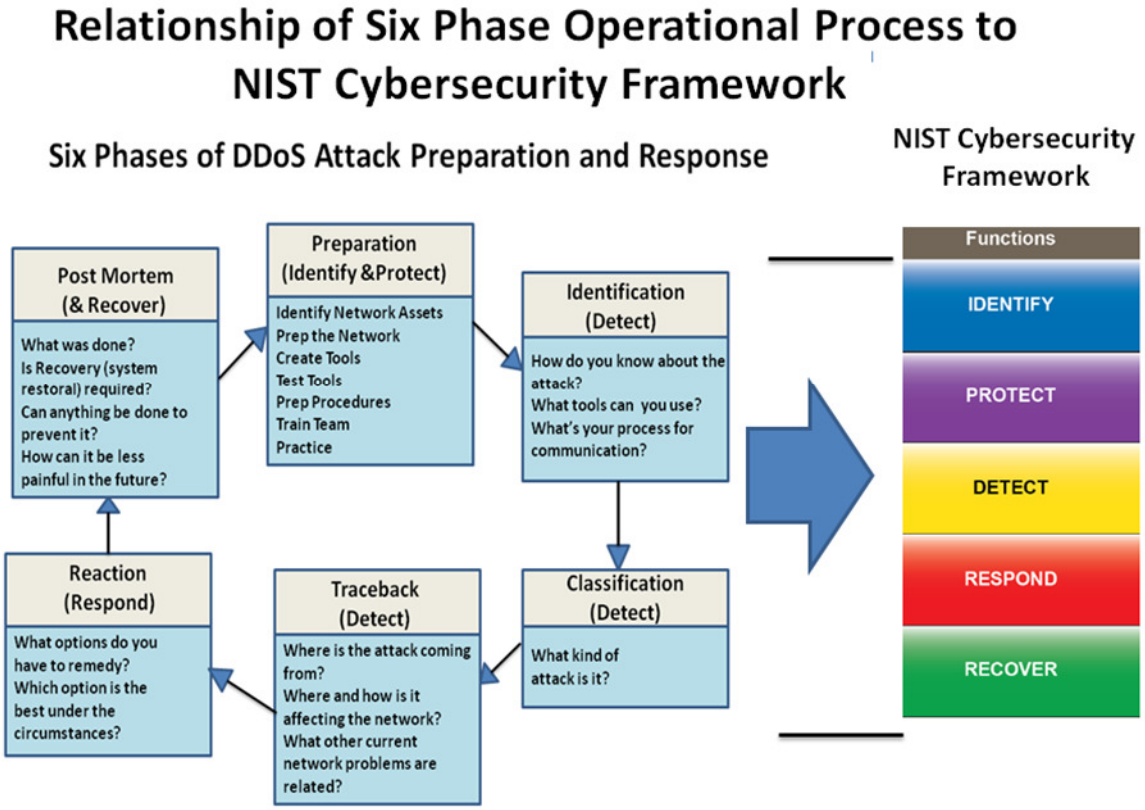
Interim Report

Methodology

- WG5 identified subgroups to focus on case studies and identification of server-based BPs
  - ISPs, Financial Community, Internet Security Experts, and Best Practices Review subgroups
- WG5 held biweekly conference calls and two face-to-face meetings to execute CSRIC charge
- WG5 reviewed in excess of 600 BPs, performed a gap analysis, and identified approximately 30 BPs to address server-based DDoS attack remediation (Appendix E)

Interim Report

WG5 Applied Six Phase Model (adaptation of Arbor Networks' model)



Interim Report

Key Findings

1. DDoS attacks are becoming large enough to overwhelm a single ISP's ability to absorb.
2. Server based attacks harness data center computational and networking resources to stage DDoS attacks of unprecedented volume.
3. Because of the increased volume of DDoS attacks, collateral damage (impacts to others not targeted by DDoS attack) is common – packet loss, delays, high latency for Internet traffic of uninvolved parties whose traffic simply happens to traverse networks saturated by these attacks.
4. DDoS attacks are being used not only to disrupt services, but to distract security resources while other attacks are being attempted, e.g., fraudulent transactions.
5. Adaptive DDoS attacks are prevalent. Attackers vary attack traffic on the fly to avoid identification and to challenge and confuse mitigation strategies.
6. Reflective and amplification attacks are still common, leveraging misconfigured DNS, NTP, and other network resources with the ability to spoof (forge) source (target) IP addresses.

Interim Report

Key Findings (cont.)

7. The botnet architecture is becoming more sophisticated and difficult to trace and C2 command and control systems are increasingly tiered using proxy servers and peer to peer networking to obfuscate the location of the system that is executing the commands. Additionally, some botnets have the ability to impair a compromised system after it has completed an attack.
8. Devices are increasingly spread out globally making the coordination of shutting down these systems difficult due to the fact that countries often have different and sometimes conflicting laws.
9. DDoS traffic builds quickly so automated mitigation capabilities are needed to protect the infrastructure.
10. Anti-spoofing (anti-forging) technologies need to be more widely deployed to protect against amplification attacks.
11. DDoS mitigation capability needs to be deployed throughout the network since it is difficult to predict where the attack will originate.

Interim Report

Key Findings (cont.)

12. DDoS mitigation requires multiple tools. ISPs need destination blackhole filtering capability to protect their networks recognizing that blackhole filtering completes the DDoS attack to the target. Attack mitigators need multiple types of less intrusive capabilities to minimize the effectiveness of DDoS attacks.
13. DDoS attacks need to be addressed by the entire networking ecosystem, not just the Network Operator. This includes hosting center and data center providers, the DDoS targets, software vendors, open source organizations as well as equipment manufacturers (the entire supply chain)..
14. DDoS mitigation requires close cooperation of targets, the network operator, and the network operators.
15. As new DDoS mitigation techniques become more effective, attackers will continue to adapt their techniques to find new ways to attack their targets.

Interim Report

Conclusions

- In this interim report we have reported progress to date, including draft recommendations and draft best practices to address server-based DDoS attacks, and indicated future activities that are required to complete our work.
- We conclude in this interim report that action will be required, not only by network operators, but by the entire ecosystem of stakeholders impacted by server-based DDoS attacks, in order to prevent, detect, and mitigate the attacks.

Interim Report

Draft Recommendations

1. FCC encourage ISPs to consider voluntary implementation, in a prioritized manner, of the recommended best practices and new recommendations (Appendix E) to address server-based DDoS attacks by promoting awareness and benefits of these best practices.
2. FCC work with appropriate parties to encourage development of best practices for Hosting Center operators and other ecosystem stakeholders concerning safe computing practices, reduced vulnerabilities, and to reduce the threat of exploited vulnerabilities, thereby reducing the incidence of server-based DDoS attacks at the point of origination.
3. FCC to encourage voluntary, private sector relationships, to the extent they do not exist already, between peers to collaborate on DDoS response best practices and mitigation support.

Interim Report

Draft Recommendations (cont.)

4. FCC charge a future CSRIC working group with the development of potential success measures to determine the effectiveness of voluntary best practices applicable to ecosystem stakeholders who are implementing them.
5. FCC encourage the development of a voluntary central clearing house for DDoS mitigation information within the existing DHS information sharing structure that can be shared among ISPs and governments to mitigate DDoS attacks in real time.
6. FCC encourage the sharing of DDoS mitigation best practices, threat, vulnerability, and incident response actions among network service providers in the Comm-ISAC.

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
  - – July 29th - scheduled
- June 13, 2014 – WG5 Interim Report
  - – comments requested NLT July 11th
- September 24, 2014 – WG5 Final Report

Next Steps

- Review and incorporate feedback on Interim Report
- Complete the Best Practices section (Appendix E)
- Perform gap analysis for additional recommendations
- Address remaining WG5 Final Report areas
  - Metrics Framework
  - Barriers to Implementation
  - BP Implementation Priority
- Continue bi-weekly conference calls
- Hold third face-to-face meeting in preparation for Final Report
- Provide periodic status updates to Steering Committee and Council