Working Group 5: Remediation of Server-Based DDoS Attacks

Status Update

September 24, 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 40 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

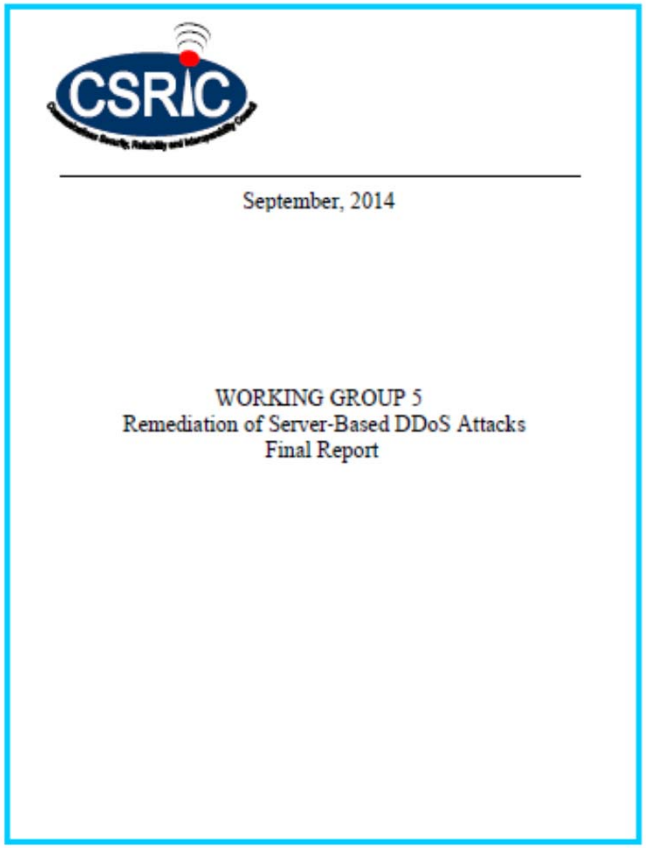
Name	Organization	Name	Organization	Name	Organization
Peter Fonash (Co-Chair)	DHS	David Fernandez	Prolexic Technologies	Wayne Pacine	Fed Reserve Board of Governors
Mike Glenn (Co-Chair)	CenturyLink	Mark Ghassemzadeh	ACS	Glen Pirrotta	Comcast
Paul Diamond (Co-Editor)	CenturyLink	Darren Grabowski	NTT	R.H. 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	Errol Weiss	FSSCC
John Denning	FSSCC	Chris Morrow	Google	Pam Witmer	PA PUC
Roland Dobbins	Arbor Networks	Mike O'Reirdan	MAAWG		
Martin Dolly	ATIS	Eric Osterweil	VeriSign, Inc.		

WG5 Status

- WG5 held a 1-day face-to-face meeting in July, hosted by CenturyLink (Arlington, VA)
  - reviewed draft final server-based DDoS attack remediation best practices, barriers to implementation, and findings and recommendations to be included in the Final Report
- WG5 delivered its Final Report Sept 22nd

Final Report

Table of Contents



September, 2014

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

Final Report

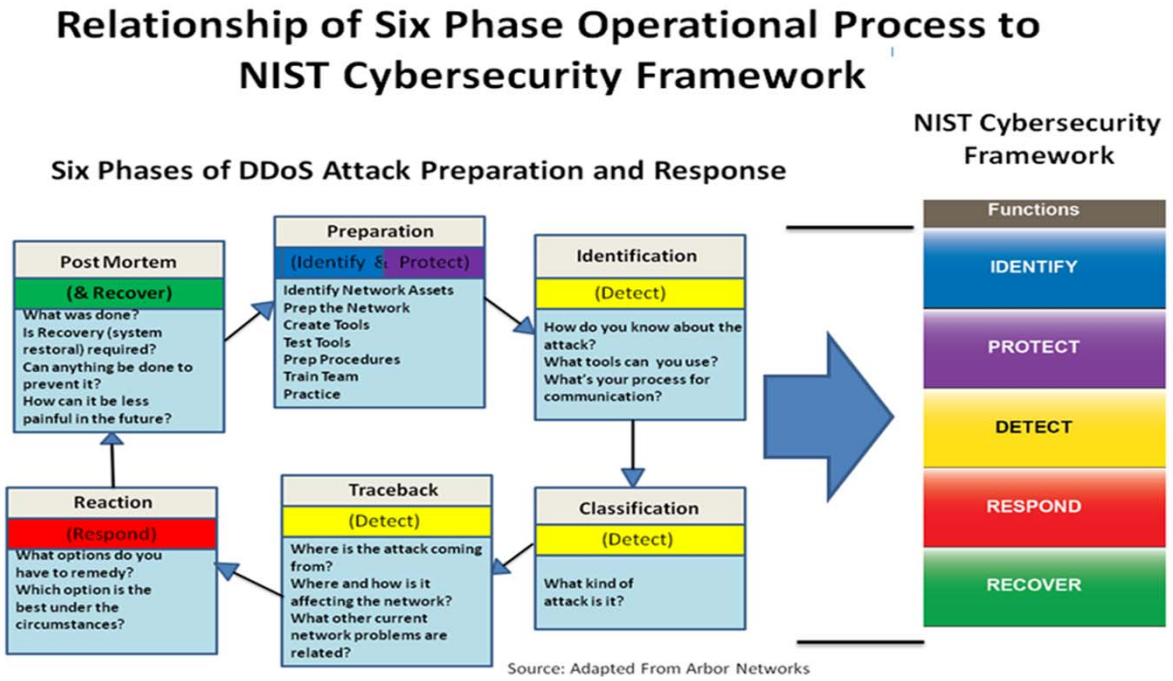
Methodology

- 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 three face-to-face meetings to execute CSRIC charge
- WG5 reviewed in excess of 600 BPs, performed a gap analysis, and identified 50 BPs to address server-based DDoS attack remediation (Appendix E)

Final Report

Methodology (cont.)

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



Final Report

Appendix E Best Practices

- WG5 reviewed in excess of 600 BPs, performed a gap analysis, and identified 50 BPs to address server-based DDoS attack remediation (Appendix E)
- BPs by the numbers…

	NIST Cybersecurity Framework Functions					Implementation Effectiveness			Implementation Difficulty			Sweet Spot
	Identify	Protect	Detect	Respond	Recover	High	Medium	Low	Low	Medium	High	High/Low
Network Operators	0	16	6	1	2	12	9	4	3	10	12	1
Hosting Providers	0	9	4	2	2	6	6	5	3	6	8	2
Targets	0	5	1	0	2	3	5	0	1	1	6	1
Sub Totals	0	30	11	3	6	21	20	9	7	17	26	4

- DDoS prevention and mitigation is a shared responsibility between the network operators, hosting providers, targets and other members of the Internet ecosystem.

Final 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.

Final Report

Key Findings (cont.)

7. The botnet architecture is becoming more sophisticated and difficult to trace and command and control (C^2) 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. In order to support automated mitigation capabilities, a standardized taxonomy to express information required to mitigate DDoS server-based attacks needs to be followed.
11. Anti-spoofing (anti-forging) technologies need to be more widely deployed to protect against amplification attacks.

Final Report

Key Findings (cont.)

12. DDoS mitigation capability needs to be deployed throughout the network since it is difficult to predict where the attack will originate.
13. 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.
14. DDoS attacks need to be addressed by the entire networking ecosystem, not just the Network Operators. 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).

Final Report

Key Findings (cont.)

15. DDoS mitigation requires close cooperation of targets, Hosting Providers, and the Network Operators. As new DDoS mitigation techniques become more effective, attackers will continue to adapt their techniques to find new ways to attack their targets.
16. The development of potential success measures to determine the effectiveness of following voluntary server-based DDoS attack best practices must be addressed not only by Network Operators, but by the broader Internet ecosystem stakeholders in order to provide meaningful, holistic interpretations of effectiveness.

Final Report

Conclusions

- Working Group 5 has documented its findings, made recommendations, suggested best practices to address server-based DDoS attacks, addressed barriers to implementation, and suggested a path forward to holistically address measures of effectiveness for following the recommended BPs.
- We conclude in this final 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.

Final Report

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 encourage the development of best practices for Hosting Providers to promote safe computing practices, reduce vulnerabilities, and reduce the threat of exploiting vulnerabilities, thereby reducing incidence of server-based DDoS attacks.
3. FCC 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.

Final Report

Recommendations (cont.)

4. FCC encourage the development of a voluntary central clearing house for DDoS mitigation information within the existing DHS information sharing structure that can be a resource among ISPs, Hosting Providers, targets, response organizations (CERTS & ISACs) and governments to mitigate DDoS attacks in real time.
5. FCC encourage ecosystem stakeholders to share DDoS server-based attack information between themselves or through a centralize clearing house using a standardized taxonomy, such as the Structured Threat Information eXpression (STIX) or a similar construct, to assist in automated mitigation of the attacks.
6. FCC encourage the sharing of DDoS mitigation best practices, threat, vulnerability, and incident response actions among Network Operators in the Comm-ISAC.