



June 18, 2014

DRAFT

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

Table of Contents

1	Results in Brief.....	3
1.1	Executive Summary	3
2	Introduction	3
2.1	CSRIC IV Structure	9
2.2	Working Group 5 Team Members	9
3	Objective, Scope, and Methodology	10
3.1	Objective	10
3.2	Scope	10
3.3	Methodology.....	11
4	Background	12
5	Analysis, Findings and Recommendations	13
5.1	Analysis.....	13
5.2	Findings.....	15
5.3	Conclusions	16
6	Recommendations	16
7	Appendices	16

DRAFT

1 Results in Brief

1.1 Executive Summary

Critical infrastructure sectors have been under assault from a barrage of DDoS attacks some of which have emanated from data centers and hosting providers.¹ DDoS attacks originating from data centers and hosting providers are especially problematic because of the high bandwidth and computational resources available to an attacker. This makes prevention, detection, and mitigation more important, yet more difficult. This Working Group examined and has made draft recommendations to the Council regarding network level best practices and other measures that communications providers and the FCC can take to mitigate the effects of DDoS attacks from large data centers and hosting sites. These recommendations include technical/operational methods and procedures to facilitate stakeholder implementation of the recommendations. While this report is focused on communications providers, it should be noted that it will require actions taken across the internet ecosystem, including actions by hosting providers, equipment suppliers, owners and operators of critical infrastructure, other stakeholders who rely on the internet, and even potentially end users themselves to successfully mitigate DDoS attacks.

Working Group 5 has provided recommended measures that 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 infrastructure sectors.² The recommended measures are mainly in the form of server-based DDoS mitigation Best Practices found in Appendix E. In addition, several actionable draft recommendations from Working Group 5 for the Council to consider recommending to the FCC are included here to further the work to prevent, detect, and mitigate server-based DDoS attacks.

Going forward from this interim report milestone, the Working Group 5 will assess the ISPs' level of effort in implementing the best practices (BPs) compared with the impact of implementing specific best practices to determine the subset of best practices that have a high impact but relatively low level of effort to implement. The working group will also focus on identifying any barriers to implementation of the BPs based upon the lessons learned from the ISP, Internet Security Experts, and Financial Community subgroups' case studies as well as other barriers based on the members' actual experiences with mitigating DDoS attacks. The working group will also develop a taxonomy for use in applying the best practices. Finally, the group will address initial recommendations on potential effectiveness measures aimed at measuring successful outcomes of the voluntary network level efforts to mitigate server-based DDoS attacks. The Working Group will deliver their Final Report, addressing the above items, in September 2014.

2 Introduction

This interim report documents the efforts undertaken by CSRIC IV WG5 and provides recommended measures that communications providers can take to mitigate server-based DDoS attacks launched from servers typically based in data centers and hosting providers. The interim

¹ <http://www.eweek.com/security/ddos-attacks-on-major-banks-causing-problems-for-customers/>

² <http://www.dhs.gov/critical-infrastructure-sectors>

report also provides draft recommendations for Council consideration regarding actions the FCC can take to assist in mitigating the occurrence and impact of server-based DDoS attacks.

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. CSRIC IV WG5 efforts leveraged and complement other botnet activities, including:

- CSRIC II and III DDoS Mitigation Recommendations
- Messaging, Malware, Mobile Anti-Abuse Working Group (M³AAWG)
- Online Trust Alliance (OTA) Anti-Botnet Working Group
- Cloud Security Alliance (CSA)
- Industry Botnet Group (IBG)

Working Group 5 considered the basic structure of a typical DDoS attack, and the differing types of DDoS attacks seen in the current network environments. Figure 1 shows an illustrative server-based DDoS attack. Recent DDoS attacks have exploited vulnerabilities in web-hosting companies and other large data centers to launch DDoS attacks on computer systems and websites. These attacks can originate domestically or internationally with domestic or international targets. Prevention, detection, and mitigation of these attacks is complex requiring cooperation and information sharing among ISPs and network providers, data centers and hosting providers, infrastructure manufacturers (i.e., the supply chain), and critical infrastructure owners and operators. The working group used the ecosystem interaction described above as a basis for deciding which case studies would be undertaken and which attendant industry best practices would be considered for this mitigation task addressing server-based DDoS attacks.

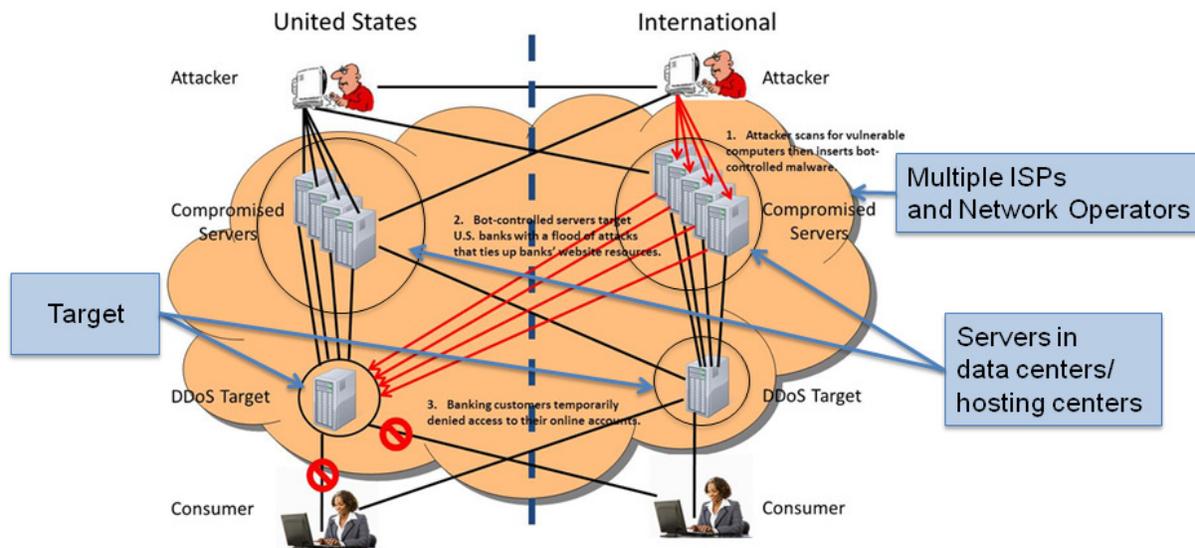


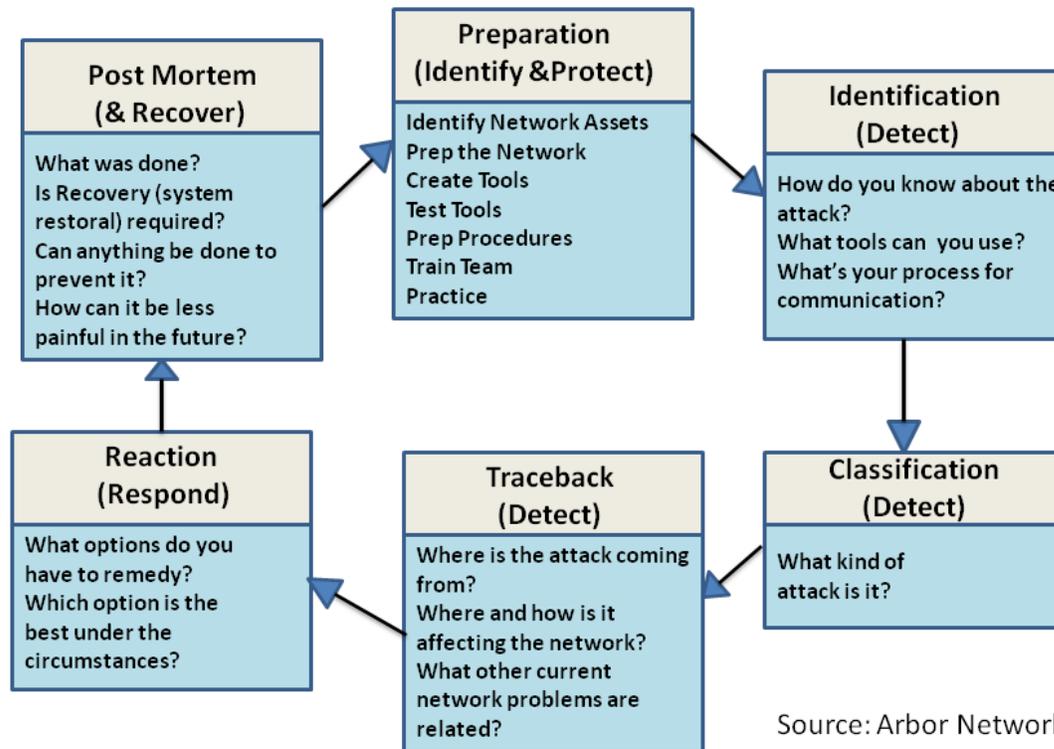
Figure 1 - Example of Server Based DDoS Attack

1

Working Group 5 also performed a gap analysis to determine where best practices were missing but required in order to align with the phases of an ISP's incident response life-cycle in protecting and responding to server-based DDoS attacks. Where gaps were identified, the working group made or will make recommendations for new best practices.

Working Group 5 is also applying the incident response life cycle as a way to map DDoS best practices and recommendations. It is expected that this mapping, along with prioritized recommendations in each area, will help ISPs identify the most important and effective best practices and recommendations in each area. We have renamed the former "Incident Life-Cycle" to "The Six Phases of DDoS Attack Preparation and Response" for the purposes of this interim report.

Six Phases of DDoS Attack Preparation and Response



In conjunction with the Six Phases model, a taxonomy of activities (Appendix A) was created in order to provide guidance on how best practices could be used in each phase. The Six Phases model is an attack preparation and response method consistent with the NIST Cybersecurity Framework. The Six Phases operational model relates to the NIST Cybersecurity Framework as follows: The Preparation Phase implements the Identify Function to identify network assets to be protected and provides the Protection Function by preparing the network and creating DDoS detection and mitigation tools. The Identification, Classification, and Traceback phases relate to the Detect Function. The Reaction Phase relates to the Respond Function, and the Post Mortem Phase to the Recover Function. This relationship is shown via Figure 2:

Relationship of Six Phase Operational Process to NIST Cybersecurity Framework

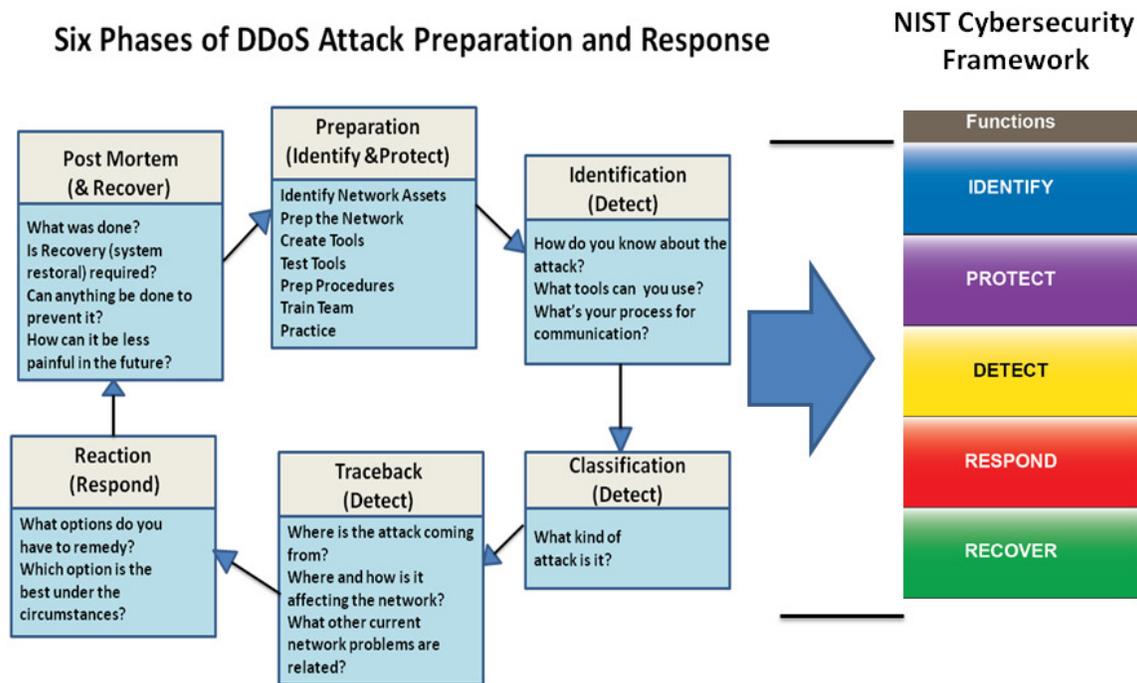


Figure 2.

For the purposes of the analysis, the working group used the following definition of a DDoS Attack: “a **denial-of-service (DoS)** or **distributed denial-of-service (DDoS)** attack is an attempt to prevent legitimate users from accessing information or services³ (US-CERT).” A distributed denial of service attack consists of two or more systems or attackers engaged in the attack at the same time to the same target. The following are types of DDoS attacks:

- Volumetric Attacks
 - Direct Packet Flooding
 - Compromised, remote control computers (bots) send attack traffic directly to the victim trying to fill the circuits with bad traffic.
 - Hundreds to tens of thousands of bots can participate.
 - Standard ISP tools handle most of these types of attacks fairly well.
 - Packets can be either spoofed or not spoofed.
 - Reflective Amplification Attacks
 - Bots spoof their source IP address to be the IP address of the victim.
 - Send traffic to services where the response will be much greater than the question.
 - DNS and NTP servers are great amplifier for these types of attacks.

³ <http://www.us-cert.gov/ncas/tips/ST04-015>

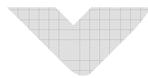
- Amplification factors of 200+ times are possible.
- Packets must be spoofed.

- Application Layer Attacks
 - Malicious software on bots is tailored to send traffic to the webserver or other application server that appears to be from a legitimate customer and consumer's significant computer resources.
 - Lower traffic volumes.
 - More work required of the attackers to achieve their goals.
 - Encrypted traffic more difficult to mitigate.
 - Full mitigation needs to look at unencrypted packets. Some mitigation can occur with encrypted packets only
 - Packets generally cannot be spoofed.
 - Domain Name Service (DNS) Attacks
 - DNS is one of two critical services on the Internet, without which almost all Internet applications fail (mail, web, etc). DNS is the white pages for the Internet.
 - Instead of attacking the victim directly, the attackers will attack the victim's externally facing or ISP DNS services, taking down the victim's traffic.
 - The attack not only affects the victim's traffic, but can affect many other ISP customers even though they may not be the target of the attack.

- State Exhaustion Attacks
 - Devices that keep state on connections such as servers, firewalls, and intrusion detection/prevention systems that have limited state capabilities.

- Control Plane Attacks
 - Routing protocols such as Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF).

The working group used the above attack types in identifying server-based DDoS attack mitigation best practices as well as discussed general mitigation tools and techniques for those attacks in forming a framework for our recommendations.



2.1 CSRIC IV Structure

Communications Security, Reliability, and Interoperability Council (CSRIC) IV									
CSRIC Steering Committee									
Chair or Co-Chairs: Working Group 1	Chair or Co-Chairs: Working Group 2	Chair or Co-Chairs: Working Group 3	Chair or Co-Chairs: Working Group 4	Chair or Co-Chairs: Working Group 5	Chair or Co-Chairs: Working Group 6	Chair or Co-Chairs: Working Group 7	Chair or Co-Chairs: Working Group 8	Chair or Co-Chairs: Working Group 9	Chair or Co-Chairs: Working Group 10
Working Group 1: Next Generation 911	Working Group 2: Wireless Emergency Alerts	Working Group 3: EAS	Working Group 4: Cybersecurity Best Practices	Working Group 5: Server-Based DDoS Attacks	Working Group 6: Long-Term Core Internet Protocol Improvements	Working Group 7: Legacy Best Practice Updates	Working Group 8: Submarine Cable Landing Sites	Working Group 9: Infrastructure Sharing During Emergencies	Working Group 10: CPE Powering

Table 1 - Working Group Structure

2.2 Working Group 5 Team Members

Working Group 5 consists of the members listed below.

Name	Company
Peter Fonash (Co-Chair)	DHS
Michael Glenn (Co-Chair)	CenturyLink
Paul Diamond (Co-Editor)	CenturyLink
Robert Thornberry (Co-Editor)	Bell Labs, Alcatel-Lucent
Vernon Mosley (FCC Liaison)	FCC
Jared Allison	Verizon
Don Blumenthal	Public Interest Registry
Chris Boyer	AT&T
Matt Carothers	Cox Communications
Roy Cormier	Nsight
Dave DeCoster	Shadowserver
John Denning	Bank of America
Roland Dobbins	Arbor Networks
Martin Dolly	ATIS
David Fernandez	Prolexic Technologies
Mark Ghassemzadeh	ACS
Darren Grabowski	NTT
Sam Grosby	Wells Fargo
Rodney Joffe	Neustar
John Levine	CAUCE
Gregory Lucak	Windstream
John Marinho	CTIA
Dan Massey	IEEE
Ron Mathis	Intrado
Bill McInnis	Internet Identity
Chris Morrow	Google
Michael O'Reirdan	MAAWG
Eric Osterweil	VeriSign, Inc.
Wayne Pacine	Fed Reserve Board of Governors
Glen Pirrotta	Comcast
R.H. Powell	Akamai
Nick Rascona	Sprint

Chris Roosenraad	Time Warner Cable
Craig Spiezle	Online Trust Alliance
Joe St Sauver	Univ of Oregon/Internet2
Kevin Sullivan	Microsoft
Bernie Thomas	CSG International
Matt Tooley	NCTA
Jason Trizna	Amazon Web Services
Errol Weiss	Citibank
Pam Witmer	PA Public Utility Commission

Table 2 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective

This Working Group was charged with examining and making 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. Our objective was to organize a working group with a wide range of experience and expertise, and include both government and industry participants. The Working Group 5 Objectives⁴ are:

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.



3.2 Scope

There has been a rapid increase in the volume, size, and scope of DDoS attacks for several years which have created challenges for Internet Service Providers due to the increased volume seen in

⁴ http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_IV_Working_Group_Descriptions_5_7_14.pdf

their networks. Recent attacks have relied on infected tenants within large data hosting centers.⁵ In order to address the server-based DDoS attack problem, Working Group 5 employed a holistic approach (e.g., multiple stakeholders represented across the ecosystem) with a focus on the actions that Network Operators could take to prevent and mitigate DDoS attacks. The holistic approach was needed since the causes and impacts of DDoS attacks need to be addressed by the entire network and hosting ecosystem in order to be effective. Addressing this attack vector has become a priority across all the ecosystem stakeholders.

WG5's approach was to be as inclusive as possible without repeating or duplicating efforts undertaken by other groups addressing other aspects of the server-based DDoS attack problem. Also, WG5's approach was to focus on efforts which would result in recommended actions specifically toward server-based DDoS attacks, i.e., many best practices reviewed were recognized as being valuable, were good best practices *in general*, but not specific to server-based DDoS attacks and so were not included here. One exception was for recommendations to protect against Domain Name System (DNS) Denial of Service attacks. Repeated and recent DNS attacks have been especially egregious, thus mitigation best practices were included in WG5's work.⁶

3.3 Methodology

Working Group 5 began by identifying subgroups to appropriately focus on case studies of server-based DDoS attacks and industry best practices analysis. The following four subgroups resulted from that focus: ISPs, Financial Community, Internet Security Experts, and Best Practices subgroups.

The Best Practices subgroup identified applicable BPs for DDoS server-based attacks while the ISPs, Financial Community, and Internet Security Experts subgroups developed representative case studies for server-based DDoS attacks. The WG5 at large then associated network level best practices to each subgroup area as well as other measures to mitigate the effects of DDoS attacks from large data centers and hosting sites.

WG5 held biweekly conference calls with its working group members to accomplish the tasking. Additionally, the subgroups held biweekly conference calls to solicit input and review their case study deliverables. WG5 held a two-day face-to-face meeting in January 2014 (Washington D.C.), and in April 2014 (Longmont, Colorado) to facilitate discussion on the deliverables.

Working Group 5 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). The group reduced the applicable list to approximately 30 salient BPs. The working group conducted a gap analysis using The Six Phases of DDoS Attack Preparation and Response in parallel with the NIST Cybersecurity Framework. Based on the gap analysis, the working group has also written several new BPs for voluntary adoption by the communications industry. Finally, the group has begun to formulate recommendations to the FCC in terms of actions the FCC can take to help mitigate the effects of DDoS attacks by enabling broader adoption of the recommended

⁵ <http://www.darkreading.com/attacks-and-breaches/bank-attackers-used-php-websites-as-launch-pads/d/d-id/1107833?>

⁶ <http://www.pcworld.com/article/2040766/possibly-related-ddos-attacks-cause-dns-hosting-outages.html>

server-based DDoS best practices.

The working group will now focus on identifying barriers to implementation of the BPs based upon the experiences summarized in the subgroup case studies, as well as member experience, and investigate outcome-based measures of effectiveness that demonstrate whether or not the voluntary efforts towards server-based DDoS attacks are having a favorable effect. The group will also apply the Six Phases taxonomy (Appendix A) as a guide in identifying candidate best practices for implementation.

4 Background

Prior CSRICs have recommended Best Practices that could be used to mitigate DoS and DDoS attacks. CSRIC II approved WG8's recommendations from their final report *ISP Network Protection Practices*:

- Recommended best practices (BPs) in areas of prevention, detection, notification, mitigation, and privacy considerations
- Focused on 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 nonresidential context.

CSRIC II also approved the WG2A's recommendations from their final report *Cyber Security Best Practices*:

- Updated Cyber Security Best Practices reflective of the current technology environment within the Communications' Industry, and related references by:
 - Analyzing existing NRIC, NIST, SANS, IEEE, etc. best practices related to Cyber Security
 - Recommending modifications and deletions to those existing Best Practices
 - Identifying new Cyber Security Best Practices across existing and relatively new technologies within the Communication industry.

CSRIC III 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 devices
- 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 botnet mitigation activities

CSRIC III approved the WG4's recommendations from their final report *DNS Best Practices*:

- Focused on Best Practices to secure DNS and routing system for the Internet during the period leading up to the implementation of DNSSEC.

CSRIC III also approved the WG5's recommendations from their final report *DNSSEC Implementation Practices for ISPs*

- To examine best practices for deploying and managing the Domain Name System Security Extensions (DNSSEC) by Internet service providers (ISPs).
- Recommend proper metrics and measurements that allow for evaluation of the effectiveness of DNSSEC deployment by ISPs.

Recent DDoS attacks have exploited vulnerabilities in web-hosting companies and other large data centers to launch DDoS attacks on computer systems and websites.⁷ CSRIC IV recognized that work in this area is both timely and important in order to impact these latest DDoS threats. Based upon the progress made in the prior CSRICs focused on residential networks, CSRIC IV WG5 was given the charter to recommend 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 infrastructure sectors.

5 Analysis, Findings, and Conclusions

5.1 Analysis

The case studies looked at a number of server-based DDoS attacks. An attack can involve multiple ISPs and multiple data and hosting centers.

- Anatomy of a Server Based DDoS Attack

As shown in Figure 3, an attacker can gain control of data center and hosting servers and leverage the sizable computational and network resources to launch a DDoS attack on an enterprise victim. Note that the target could also be part of the ISPs' infrastructure. This attack overwhelms access to the target, denying access from legitimate users as well as causing collateral damage by affecting other parties along the DDoS traffic path. Mitigation of this type of attack requires action by all the parties involved:

- Multiple ISPs
- Hosting Providers / Data Centers / Resellers
- Target infrastructure
- ISP infrastructure of the originating attacker

⁷ <http://www.darkreading.com/attacks-and-breaches/bank-attackers-used-php-websites-as-launch-pads/d/d-id/1107833?>

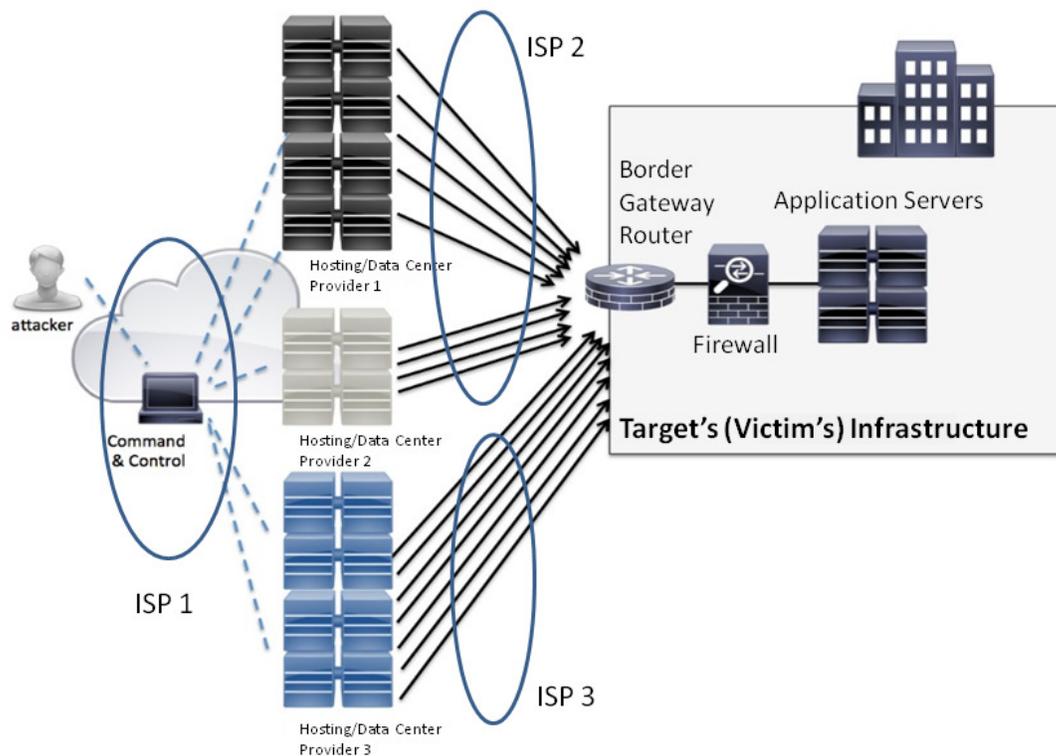


Figure 3 – A Server Based DDoS Attack

Source:

http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html#_Toc374453043

- Attack Taxonomy – A Taxonomy of the types of server-based DDoS attacks was created in order to determine the scope of defenses that would be needed to mitigate the attacks. The attack taxonomy is contained in Appendix C.
- Case Studies
 - Working Group 5 identified three subgroups to focus attention on stakeholder server-based DDoS attack case studies and a fourth subgroup to conduct an industry best practices analysis. The subgroups were: ISPs, Financial Community, Internet Security Experts, and Best Practices subgroups.
 - The Best Practices subgroup identified applicable BPs for DDoS server-based attacks while the ISPs, Financial, and Internet Security Experts subgroups developed representative case studies for server-based DDoS attacks. The case studies are included in Appendix D.
- Recommended Best Practices
 - Draft Best Practices are included in Appendix E
- Provide implementation guidance for Best Practices – Work planned for 3Q2014

- Investigate Barriers to best practice implementation – - Work planned for 3Q2014
- Investigate Measures of Effectiveness – - Work planned for 3Q 2014
- Investigate the feasibility of using STIX/TAXII for real time DDoS attack information sharing.

5.2 Findings

Key Findings from Case Studies:

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.
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.
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.

5.3 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.

6 Recommendations

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.
- 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's 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.

7 Appendices

Appendix A: Six Phases of DDoS Attack Preparation and Response Taxonomy

Appendix B: Server-Based DDoS Glossary

Appendix C: DDoS Attack Taxonomy

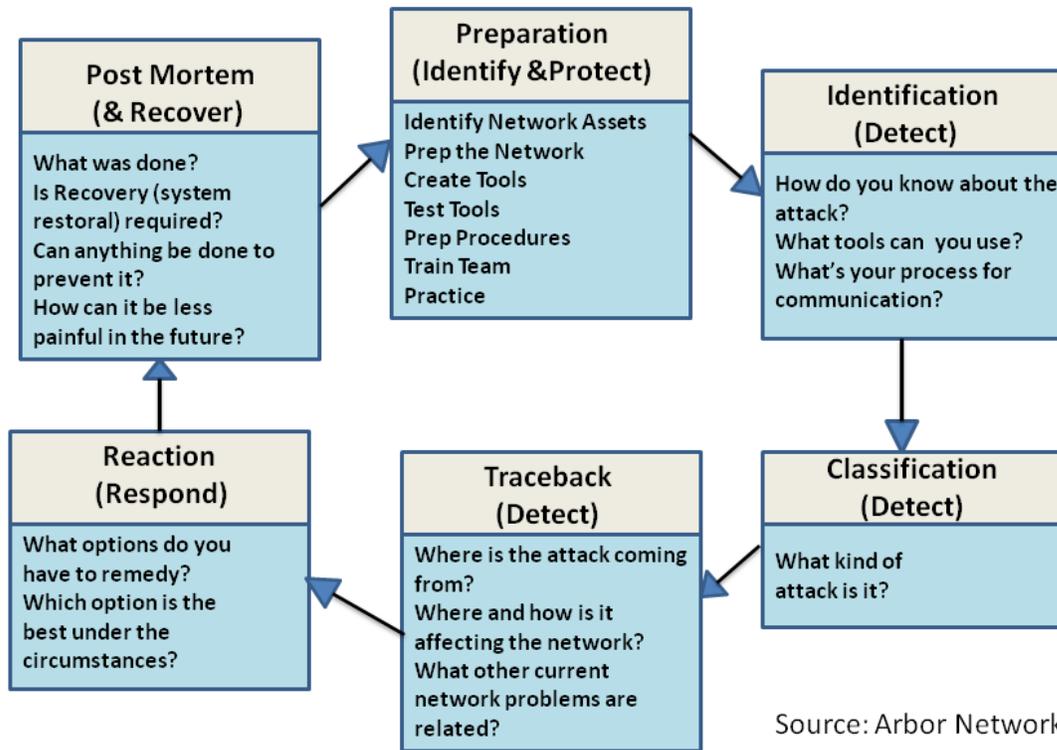
Appendix D: DDoS Attack Mitigation Case Studies

Appendix E: Server-Based DDoS Mitigation Best Practices

DRAFT

Appendix A: Six Phases of DDoS Attack Preparation and Response Taxonomy

Six Phases of DDoS Attack Preparation and Response



Preparation

Communication

ISP

ISP to ISP
ISP to Hosting
ISP to Victim
ISP to Central Coordination Center

Hosting

Hosting to ISP
Hosting to Hosting
Hosting to Victim
Hosting to Central Coordination Center

Target

Victim to ISP
Victim to Hosting
Victim to Victim

Monitoring & Visibility

ISP

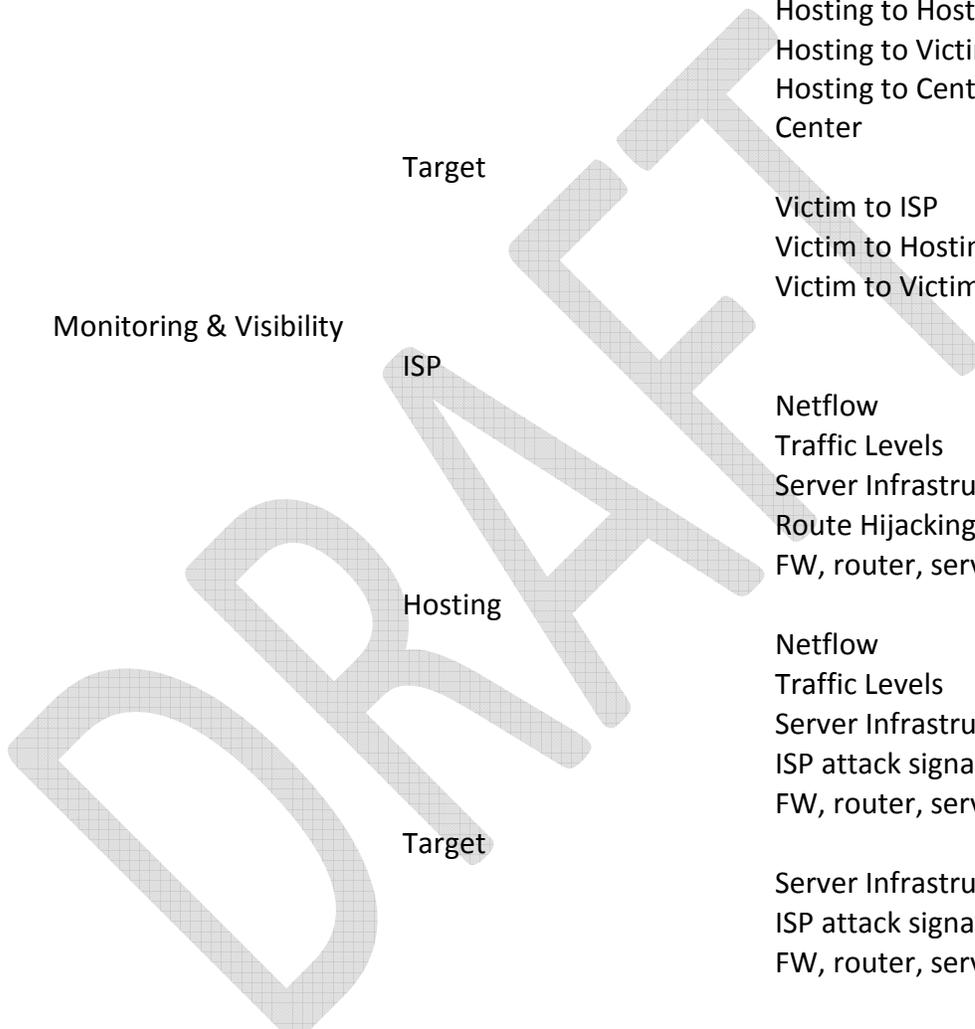
Netflow
Traffic Levels
Server Infrastructure Resource Levels
Route Hijacking
FW, router, server logs

Hosting

Netflow
Traffic Levels
Server Infrastructure Resource Levels
ISP attack signaling
FW, router, server logs

Target

Server Infrastructure Resource Levels
ISP attack signaling
FW, router, server logs



Prevention

ISP

Anti-spoofing techniques
Reduce Reflective Surfaces
Rate Limits / Traffic Blocking

Hosting

Anti-spoofing techniques
Reduce Reflective Surfaces
Rate Limits / Traffic Blocking
Server Resource Minimization Plan
and Procedures

Target

Server Resource Minimization Plan
and Procedures

Deploy and Configure
Mitigation Tools

ISP & Pure Play DDoS
Company Filtering

CDN Filtering (Web traffic attacks)
BGP Flowspec
Black Hole Filtering (Source and
Destination)
Network Data Scrubbing

Hosting Filtering

On-site data scrubbing

Target Filtering

On-site data scrubbing

Capacity and Resources

ISP

DNS server
DNS Network Capacity
BGP Link, Router and State
Protection

Hosting

DNS server
DNS Network Capacity
BGP Link, Router and State
Protection
Data Center Uplink Bandwidth
FWs, IDS/IPS, Switch capacities

Target

Server and Network Uplinks
FWs, IDS/IPS, Switch capacities
Server resource capacities

Minimize Attack Service

ISP

Close Open DNS Resolvers
Rate limit DNS queries
Rate limit open protocols (NTP, Echo,
etc)
Turn off unnecessary protocols on
network infrastructure

Hosting

Close Open DNS Resolvers
Rate limit DNS queries
Rate limit open protocols (NTP, Echo,
etc)
Turn off unnecessary protocols on
network infrastructure
Turn off unnecessary protocols on
server & virtual infrastructure

Target

Turn off unnecessary protocols on
server & virtual infrastructure

Peering and Upstream
ISP cooperative
mitigation agreements

Formal and informal
mitigation agreements
Identification of 24/7
operational contacts at
peer or upstream ISPs for
attack mitigation
assistance

DRAFT

Identification

Monitoring & Visibility

ISP

Netflow (with router and interface information)
Traffic Levels
Server Infrastructure
Route Hijacking
FW, router, server logs
Full Packet Capture and Analysis

Hosting

Netflow (with router and interface information)
Traffic Levels
System loads
ISP attack signaling
FW, router, server logs
Full Packet Capture and Analysis

Target

System loads
ISP attack signaling
FW, router, server logs
Full Packet Capture and Analysis

Confirm with target (customer) that the traffic is truly attack traffic.

Classification

Type of attack

Volumetric Attack?

Direct Packet Flood
Reflection/Amplification

Application Layer Attack?

State or Resource
Exhaustion Attack?

Control Plane Attack?

Ipv6 Specific Attack?

Traceback

Identification of source
IPs

Identification of ingress
router interfaces

Identification of DDoS
Packet Paths

Intermediate traffic loads

Identification of Reflective
Surface (routers, servers,
etc)

Identification of ingress router
interfaces for spoofed reflective
packets

Reaction

Determine best tool or set
of tools to mitigate the
attack

Analyze residual traffic
going to target fine tune
mitigation filters and
changes in attack traffic
and methods

Monitor filtering methods
to minimize false positive
traffic errors

Is help needed from peer
or upstream providers to
mitigate the attack?

Post Mortem

How quickly was the attack identified and classified?

Were the tools effective in mitigating the attack?

Are there any additional preventative measures that can be put in place to prevent future attacks?

Are there any additional mitigation measures that can be put in place to more effectively mitigate future attacks?

Were communications timely and effective?

Were mutual ISP assistance agreements needed? Effective?

Appendix B: CSRIC IV WG5 Server-Based DDoS Glossary

(This glossary combines glossaries from CSRIC III WG7 Final Reports as a baseline.)

I. Terms:

1. Bot

The following definition draws heavily from "Recommendations for the Remediation of Bots in ISP Networks" (Referenced in Appendix 2):

A malicious (or potentially malicious) "bot" (derived from the word "robot", hereafter simply referred to as a "bot") refers to a program that is installed on a system in order to enable that system to automatically (or semi-automatically) perform a task or set of tasks typically under the command and control of a remote administrator (often referred to as a "bot master" or "bot herder.")

Computer systems and other end-user devices that have been "botted" are also often known as "zombies".

Malicious bots are normally installed surreptitiously, without the user's consent, or without the user's full understanding of what the user's system might do once the bot has been installed.

Bots are often used to send unwanted electronic email ("spam"), to reconnoiter or attack other systems, to eavesdrop upon network traffic, or to host illegal content such as pirated software, child exploitation materials, etc.

Many jurisdictions consider the involuntary infection of end-user hosts to be an example of an unlawful computer intrusion.

2. Botnet

Botnets are networks of Internet-connected end-user computing devices infected with bot malware, which are remotely controlled by third parties for nefarious purposes.

A botnet is under the control of a given "bot herder" or "botmaster." A botnet might have just a handful of botted hosts, or millions.

3. Communication Provider

Communications Providers consist of Internet Service Providers, Service Providers, Network Operators, Hosting Center Operators, Data Center Operators, and the manufacturer ecosystem that supports these providers.

.

4. Customer (or "Direct Customer")

The party contracting with an ISP for service. Distinguish the "customer" from an "authorized user:" for example, a coffee shop might purchase Internet service from an ISP. The coffee shop would be the ISP's customer. The coffee shop might elect to offer free use of its connection (if permitted by the ISP's Acceptable Use Policy, or AUP) to those who buy coffee from it -- coffee buyers would then be authorized users of the connection purchased by the coffee shop, but not the ISP's direct customer.

5. Data Center

A facility dedicated to housing large amounts of computing and networking resources in an environment providing high availability power and networking capabilities.

6. Detection

Detection is the process whereby a service provider or end-user comes to be aware that a particular system or device has been infected with malicious software. A service provider may detect that a system has become infected many different ways, including as a result of receiving complaints from third parties about spam, network scanning, or attacks that have been sourced from that system. End-users may detect system infections through software tools or other means.

7. Ecosystem

This term is often used to describe the interrelationship of various Internet participants—the hardware manufacturers, software developers, ISPs, and providers of various Internet content, applications, and services that make the Internet work and be useful for end-users.

The internet ecosystem includes operating system vendors, end-user focused organizations, providers of Internet content, applications, and services, ISPs, search providers, end-users, IT departments, hosting companies, blog providers, security vendors, researchers, government, financial services companies, and other parties.

The so-called "underground economy" is also often described as an "ecosystem," with multiple participants filling diverse specialized roles. For example, some participants may specialize in writing malware, while others may "harvest" email addresses from web pages and mailing lists, while still others may specialize in distributing malware to those harvested email addresses. The malware ecosystem will also normally include the population of targeted potential victims, and law enforcement agencies working to combat cybercrime.

8. End-user

End-User: In a computing and networking context, the end-user is the person who ultimately makes authorized use of a product or service.

The end-user may often not be the same as the person who may have purchased the product or service. For example, a coffee shop owner may purchase connectivity for use by his or her customers; in that scenario, the coffee shop customers, and not the coffee shop owner, represent the actual "end-users," even though they did not directly contract with an ISP for the connectivity they're using.

A party, such as a hacker/cracker who makes use of a product or service without the authorization of the purchaser, would normally be considered a cyber intruder and not an "end-user" per se.

9. Hosting Center

Hosting centers offer various kinds of hosting services which may range from managed hosting utilizing computing, network, and management resources provided by the hosting center operator, to collocation hosting which allows tenants to provide their own equipment housed in

the hosting operator racks.

10. ISP

An Internet Service Provider (ISP) is a company that provides retail access to the Internet for members of the public, or for businesses and other organizations. Those connections may be via cable, DSL, satellite, wireless, dialup, or other technologies. ISPs are sometimes also known as "access providers."

An enterprise that provides access to the Internet solely for its own employees would not normally be considered to be an ISP. Likewise, a network carrier that only provides wholesale access to the Internet for other ISPs would normally be considered to be a network service provider (NSP), rather than an ISP.

11. Malware

"Malware" is short for "malicious software."

Malicious bots are one type of malware. Other forms of malware include categories of software known as viruses, Trojan horses, worms, rootkits, crimeware, keystroke loggers, dialers, spyware, adware, etc. The factors that distinguish those different types of malware are less important than an understanding of why malware may be viewed as "malicious."

Malware often violates one or more of the following fundamental principles:

- (a) Consent: Malware may be installed even though the user did not knowingly ask for that to happen.
- (b) Honesty: Malware may pretend to do one thing, while actually doing something completely different.
- (c) Privacy-Respectfulness: Malware may violate a user's privacy, perhaps capturing user passwords or credit card information.
- (d) Non-Intrusiveness: Malware may annoy users by popping up advertisements, changing web browser's home page, making systems slow or unstable and prone to crash, or interfering with already installed-security software.
- (e) Harmlessness: Malware may be software that hurts users (such as software that damages our system, sends spam emails, or disables security software).
- (f) Respect for User Management: If the user attempts to remove the software, it may reinstall itself or otherwise override user preferences.

It all adds up to "software users just don't want."

Users may unknowingly install malware by opening a tainted attachment received by email, or by visiting a web page that has malicious content. Systems may also be directly infected by a remote attacker as a result of the attackers targeting a known vulnerability that may be remotely exploitable, or by the user mounting an infected CD, DVD, or thumb drive.

12. Mitigation

Mitigation is the process of managing or controlling the effects associated with a bot. For example, if a system is infected with a spam bot, and is spewing unwanted commercial email, mitigation may consist of filtering the spam that is being emitted from that device.

Note that mitigation typically does not involve fixing the underlying condition (that would be "remediation"); mitigation just manages the symptoms associated with a condition.

13. Notification

Notification is a process whereby ISPs communicate with their end-users regarding the possible infection of the end-user's device by bot malware or how a subscriber can prevent or identify such an infection. Notification may also entail a process whereby end-users are directed to tools that will enable self-discovery of bot infections. Notification can take different forms, including direct notification by the ISP to the end-user, or indirect notification through available self-discovery tools or a third party. Notification may be done via multiple potential channels, including (but not limited to) e-mail, postal mail, a phone call, in-browser notification, web-based self-discovery tool, or SMS message.

14. Prevention

Prevention is the process of hardening a system or service so that it is less vulnerable to compromise and exploitation. For example, on many systems, prevention may involve:

- Patching the operating system and all applications with available security fixes
- Installing or enabling a firewall
- Using anti-virus software
- Making sure the system is regularly backed up
- Using strong passwords
- Disabling all unneeded network services
- Encouraging users to safely use internet services (e.g., e-mail, web browsing, etc.)

15. Remediation

Remediation is the process that an end-user goes through to clean up a botted computer so that it is no longer infected. In easy cases this may involve installing and running an anti-virus product. In more difficult cases, remediation may involve more substantial intervention up to "nuking and paving" the system -- formatting it and reinstalling it from scratch, or at least from the last known-clean backup. Once the system is clean, or has been reinstalled, it will then normally be hardened to protect it from reinfection.

16. Server

A network server is a computer designed to process requests and deliver data to client computers over a local network or the Internet. Servers in data centers and hosting centers typically have high bandwidth connections to the network and have substantial computational resources to process large numbers of requests in a short period of time.

17. Spam

Unwanted and unrequested e-mail, often commercial in nature, normally sent to a large number of recipients in substantially identical form. Spam is often sent by "affiliates" who are paid by the person running the affiliate program when recipients purchase the spamvertised product.

II. The Infection Lifecycle:

1. Clean: For the purposes of the ISP voluntary Anti-Botnet Code of Conduct, a computer or other networked device will be considered "clean" when it (a) exhibits no externally discernible symptoms of infection (such as sending spam, participating in a distributed denial of service attack, or contacting a known command and control host), and (b) a review of the computer or other networked device with a generally accepted commercial or free/open source anti-virus program (using the most recently available definitions) finds no infection, and (c) the computer or other device otherwise appears to be operating normally in all respects. A newly purchased system shall be presumed to start in a clean status "out of the box," absent evidence to the contrary.

2. Vulnerable: A computer or other networked device shall be deemed "vulnerable" when it has one or more flaws or misconfigurations that render it potentially susceptible to compromise or infection. A common example of a vulnerable device is one that hasn't been patched, or which uses an easily guessed password for access. Note that a system may be "clean" yet "vulnerable" simultaneously, as in the case where a vulnerable system is protected by a compensating control (such as a firewall), thereby allowing the system to avoid becoming infected or compromised despite the presence of one or more vulnerabilities.

3. Infected: An infected computer or infected network device is one that has had malicious software or malicious firmware installed on/in it without knowing authorization. That malicious software or malicious firmware may be called a virus, a Trojan horse, a worm, a rootkit, a keystroke logger, a dialer, crimeware, spyware, adware, etc. A full definition of "malware" can be found in the glossary appearing in Appendix A to the FCC CSRIC "ABCs for ISPs."

4. Isolated: A system that is infected or compromised may be isolated to prevent it from generating unwanted Internet traffic. Isolated hosts are often put into "walled gardens" where they are limited to accessing a strictly limited set of resources needed for remediation, or are allowed just to access life-safety services (such as VoIP telephony service for emergency use).

5. Offline: An offline system is one where no network access is allowed to/from that host whatsoever. Conceptually, think of an ethernet connected host where the ethernet cable has been disconnected (or the ethernet switch port has been disabled), although obviously different technical processes are used in the case of cable modem connections, DSL connections, wireless access, modem access, etc.

6. Disinfected: A system shall be considered "disinfected" when, having been infected, it has been returned to a "clean" state (as previously defined above). The first step in disinfecting a system is often installing and running an antivirus product (if one wasn't already installed and

up-to-date). In some cases, it may be necessary to format and reinstall the system from scratch to overcome particularly well-hidden persistent malware.

7. **Hardened:** A hardened system is one that has been systematically configured so as to eliminate the system's vulnerabilities (or potential vulnerabilities). For example, among other things, a hardened system will be patched up to date, will have all unnecessary services disabled, will require encryption of all sensitive network traffic, will use strong passwords or multifactor authentication, will do secure logging to an off-system logging host, etc.

8. **Reinfected:** A system that has been disinfected but NOT hardened will often promptly become reinfected.

9. **Compromised:** While many vulnerable systems may be compromised as a result of being infected with malware, other vulnerable systems may be compromised as a result of weak passwords or misconfigurations (such as critical files that are unintentionally able to be modified by unauthorized parties). A compromised system is not trustworthy.

10. **Managed:** A "managed host" is one that is centrally administered, rather than being self-administered by the system's user(s). Managed hosts are commonly seen in large corporations, and in government agencies.

11. **Monitored:** A monitored host is one that is continually (or at least periodically) scrutinized for things like anomalous network traffic or unauthorized changes to critical system files. Monitoring may take place via network security systems, such as Snort, or via host-based systems such as Tripwire.

12. **Replaced:** While most users will attempt to disinfect and harden an infected system, some may elect to replace that system with a new one instead. The prior system may then be sold or given to a third party, who may get the system along with any malware installed on it.

13. **Shared:** A shared system is one that's used by multiple individuals. A common example of a shared device would be a family device used by a parent or parents as well as by children or other family members. A shared device often seems to be more prone to infection (or other security issues) than a system that's used by only a single entity.

14. **Orphaned:** An orphaned device or orphaned program is an older one for which the vendor no longer releases even critical security/stability patches. Orphaned systems or programs generally cannot be hardened.

III. Ecosystem Roles

1. **Customer:** In the ABCs for ISPs context, the person who is paying an ISP for Internet service.

2. **System Owner:** The person who owns a given computer or other device.

3. **System User:** A person whom the system owner intentionally allows to use their computer or other device.

4. **Support Person:** For residential computers, a support person may be a family member or friend who helps the system owner or user to use and maintain their computer. A support person may also be a commercial computer support specialist hired for that purpose by the

computer owner or user.

5. ISP Security/Abuse Team: The person or group at an Internet Service Provider who deals with complaints about a customer.

6. Vendor: The company that manufactured and marketed a computer system or software program. One might talk about an operating system vendor, an application software vendor, a hardware vendor, or an antivirus software vendor, for example.

7. Law Enforcement: A police officer, sheriff, federal agent, or other sworn individual with the power to investigate crimes, gather evidence and make arrests.

8. Regulator: A state or federal official tasked with managing business practices or other activity so as to ensure fundamental fairness or regulatory compliance. An example of a regulator would be the U.S. Federal Trade Commission. Regulators normally employ civil sanctions (such as administrative fines or civil lawsuits) rather than criminal sanctions (such as arrest/incarceration).

9. Unauthorized User: A person who uses a computer or other device without the intentional permission of the system owner, or someone who uses authorized access in excess of their authorization.

10. Malware Author: The programmer or programming team that designs and codes a piece of malware, such as a bot.

11. Botmaster: A botmaster is a person who operates a network of botted computers, often using them to send spam or attack other computers. The botmaster normally sends commands to "his" or "her" bots via a command and control host, e.g., a server under his or her control.

12. Affiliate: In this context, an affiliate is a person who helps to market a particular product or service in exchange for compensation, typically using pay-per-impression, pay-per-click, pay-per-install, or revenue sharing models:

(a) Pay-per-impression (PPI): affiliates are typically website owners who are paid according to the number of times a web site banner or other advertisement is shown to visitors

(b) Pay-per-click: in this model, affiliates are paid when someone actually clicks on an advertisement

(c) Pay-per-install: in this model, affiliates are paid when a program supplied to them is installed on a new system, either surreptitiously or with the knowing consent of the user (perhaps as part of a "sponsored access" offer for a program or site that would otherwise need to be purchased)

(d) Revenue sharing: in this model, affiliates are paid a percentage of the sales associated with the customers they refer.

13. List Seller: A list seller is someone who compiles and distributes lists of email addresses. For example, a spammer who wants to spamvertise an illegal online casino might purchase a list of email addresses known to be associated with online gamblers.

14. Bullet Proof Hosting Company: A so-called bullet proof hosting company is one that agrees to host a web site or other online presence notwithstanding complaints that may result from that activity, typically in exchange for the hosted party paying a premium price. Bullet proof hosting

companies may be used to host spamvertised web sites, malicious software, child abuse materials, or other content likely to be unacceptable to regular hosting companies.

15. Bullet Proof Domain Name Registrars: A so-called bullet proof domain registrar is one that allows a spammer or other cyber criminal to register a domain name, and to keep that domain up, notwithstanding complaints that may be associated with that domain name. This service normally is provided for a premium over market domain name registration rates.

16. Payment Processor: When an affiliate makes a sale, payment is normally made by credit card. The entity that processes that credit card transaction is known as a "payment processor."

17. Drop Shipper: A drop shipper is an entity that manages order fulfillment for an affiliate program. For example, a drop shipper specializing in illegal pharmaceuticals may package and ship orders obtained by a pill spammer.

18. Online Currency Exchanger: Some affiliates may be paid using an online currency rather than via a mailed check or direct deposit. Online currency exchangers make it possible for some to purchase an online currency in exchange for cash, or vice versa.

19. Abuse Reporter: Third party reporting an abuse incident to an ISP, or through a clearinghouse (such as a computer security incident response team).

DRAFT

Appendix C: DDoS Attack Taxonomy

1 DDoS Attacks - Attacking Availability

1.1 Definition of DDoS Attacks

For the purposes of the analysis, the working group used the following definition of a DDoS Attack: “a **denial-of-service (DoS)** or **distributed denial-of-service (DDoS) attack** is an attempt to prevent legitimate users from accessing information or services⁸ (US-CERT).” A distributed denial of service attack consists of two or more systems or attackers engaged in the attack at the same time to the same target.

1.2 Goals of DDoS Attacks

1.2.1 Attacks Against Capacity

1.2.2 Attacks Against State

1.3 DDoS Attack Tools

1.3.1 Botnets

1.3.1.1 Client Botnets

1.3.1.2 Server Botnets

1.3.1.3 Participatory Botnets

1.3.1.4 Other Botnets

1.3.2 Attack Harnesses

1.3.3 Traffic-Generation Applications

2 IPv4 & IPv6 DDoS Attacks

2.1 Volumetric DDoS Attacks

2.1.1 Direct Packet-Flooding

2.1.1.1 ICMP & ICMPv6

2.1.1.2 UDP

2.1.1.3 TCP

2.1.1.3.1 SYN-Flood

2.1.1.3.2 RST-Flood

2.1.1.3.3 ACK-Flood

2.1.1.3.4 RST-Flood

2.1.1.3.5 Null-Flood

2.1.1.3.6 SYN/ACK Flood

2.1.1.3.7 XMAS-Tree Flood

2.1.1.3.8 Invalid Flag Combination Flood

2.1.1.3.9 Port 0 Flood

2.1.1.4 Fragmented Packets

2.1.1.4.1 UDP

2.1.1.4.2 TCP

2.1.1.5 Protocol 0

2.1.1.6 GRE (General Routing Encapsulation) flood

2.1.1.7 ESP (IPsec Encapsulating Security Payload) flood

2.1.1.8 RTP flood

2.1.1.9 Other 'Non-Standard' Protocols flood

2.1.2 Reflection/Amplification

2.1.2.1 UDP Reflection/Amplification

⁸ <http://www.us-cert.gov/ncas/tips/ST04-015>

- 2.1.2.1.1 DNS Reflection/Amplification
 - 2.1.2.1.1.1 DNS Reflection/Amplification with Open DNS Recursors & Authoritative Servers
 - 2.1.2.1.1.2 DNS Reflection/Amplification with Authoritative Servers Only
- 2.1.2.1.2 SNMP Reflection/Amplification
- 2.1.2.1.3 ntp reflection/amplification
- 2.1.2.1.4 chargen reflection/amplification
- 2.1.2.1.5 tftp reflection/amplification
- 2.1.2.1.6 RADIUS reflection/amplification
- 2.1.2.1.7 SIP reflection/amplification
- 2.1.2.1.8 Other UDP reflection/amplification attacks
- 2.1.2.2 TCP Reflection/Amplification
 - 2.1.2.2.1 SYN/ACK Reflection
 - 2.1.2.2.2 RST Reflection
- 2.2 Application-Layer DDoS Attacks
 - 2.2.1 HTTP
 - 2.2.1.1 GET
 - 2.2.1.2 POST
 - 2.2.1.3 CGI
 - 2.2.1.4 'Slow' HTTP Variants
 - 2.2.2 SSL/TLS
 - 2.2.2.1 Malformed SSL/TLS
 - 2.2.2.2 SSL/TLS Negotiation
 - 2.2.2.3 HTTP/S Encapsulated Attacks
 - 2.2.3 DNS
 - 2.2.3.1 Authoritative DNS Request Floods
 - 2.2.3.2 Recursive DNS Request Floods
 - 2.2.3.3 Authoritative zone delegation attacks
 - 2.3.4 SIP
 - 2.2.4.1 INVITE Floods
 - 2.2.4.2 INFO Floods
 - 2.2.4.3 NOTIFY Floods
 - 2.2.4.4 RE-INVITE Floods
 - 2.3.5 ssh
 - 2.2.5.1 ssh negotiation
 - 2.2.5.2 Login Brute-Forcing
 - 2.3.6 Middle-and Back-Tier Applications
 - 2.2.6.1 AAA Subsystems
 - 2.2.6.2 Databases
 - 2.2.6.3 Image Generation Systems
 - 2.2.6.4 Other Middle- and Back-Tier Applications
 - 2.2.7 Other Applications
- 2.3 State Exhaustion DDoS Attacks
 - 2.3.1 The Role of State in DDoS Attacks
 - 2.3.2 TCP Connection DDoS Attacks
 - 2.3.2.1 Connection Exhaustion
 - 2.3.2.2 Direct Connection Exhaustion
 - 2.3.2.3 Application-Layer Second-Order Connection Exhaustion

- 2.4.3 State Exhaustion in Stateful Middleboxes/Middleblades
 - 2.3.3.1 Stateful Firewalls
 - 2.3.3.2 IDS/'IPS'
 - 2.3.3.3 Load-Balancers
 - 2.3.3.4 NATs/CGNs/Proxies
- 2.4 Control-Plane DDoS Attacks
 - 2.4.1 Routing
 - 2.4.1.1 BGP4 & MP-BGP
 - 2.4.1.2 OSPF & OSPFv3
 - 2.4.2 Other Control-Plane Attacks
- 3 IPv6-Specific DDoS Attacks
 - 3.1 Extension Headers
 - 3.1.1 ICMPv6
 - 3.1.1.1 Neighbor Discovery
 - 3.1.1.2 Router Advertisement
- 4 Multi-stage attacks
 - 4.1 Flood followed by attacks of mitigation mechanisms

DRAFT

Appendix D: DDoS Attack Mitigation Case Studies

ISP Subgroup Case Studies

I. Background

Internet service providers (ISPs) have been actively mitigating *distributed denial of service (DDoS)*⁹ for a number of years. In the most common early versions of the attack, personal computers connected to home broadband services began to experience malware infections that would transform the machines into so-called *zombies* (now referred to as *bots*). Using separately compromised servers for control, attackers could then command large groups of bots to send volumes of data at some victim, usually a website. The website would then become overwhelmed with the incoming data, and would be unable to process normal authorized requests.

From roughly 1999 to 2011 the volumes of data aimed at most ISP infrastructure, and the skill with which the volumes of data were crafted by adversaries, were within manageable thresholds. *There have been very few major, service-impacting attacks on any portion of large ISPs infrastructure during that twelve-year period.* This includes attacks on major Tier 1 ISPs domain name service infrastructure. Attacks during this period were generally sized in the multiple Gigabit-per-second range.

In addition, during this same time period, some ISPs developed new managed security services for business customers to help them mitigate DDoS attacks on their own infrastructure. Several U.S. financial institutions currently subscribe to these services which typically involve real-time detection of attacks based upon either volumetric or application based solutions. For example, a DDoS attack could be detected volumetrically based upon traffic spikes using data collection tools and then redirection of the traffic using the border gateway protocol (BGP) toward specially designed firewalls that filter the attack. The scrubbed traffic is then "tunneled" to the customer site over the ISP's infrastructure.

In late 2012 ISPs started to see larger scale attacks by adversaries creating enough inbound volume to potentially overwhelm the ingress capacity for some ISP's scrubbing infrastructure. In addition the botnet triggering the attack was unique in that it utilized servers on often sizable network connections as bots, rather than compromised PCs on consumer broadband connections. Later in the third quarter, this same adversary launched a series of "telegraphed attacks" on banking websites with their warnings posted routinely on *pastebin*. These attacks reached unprecedented sizes, often again targeting DNS. In response, ISPs made several adjustments in real time to enhance their infrastructure, scrubbing platforms and DNS site capacity¹⁰.

This case study is intended to provide an explanation and proposed practices that ISPs can take

⁹ A **denial-of-service (DoS)** or **distributed denial-of-service (DDoS) attack** is an attempt to prevent legitimate users from accessing information or services⁹ (US-CERT).

¹⁰ This is an ongoing process of traffic engineering. Many ISPs continually monitor traffic flows to ensure adequate capacity. This same process applies to data links into ISPs DDoS scrubbing infrastructure.

in response to large scale DDoS attacks in the future.

II. Simplified Taxonomy of DDoS Attacks for ISPs

While the broader working group has developed a detailed taxonomy of DDoS attacks, the ISP sub-group thought it was necessary to develop a simplified version for use with the case study. The sub-group also discussed a model to classify DDoS attacks in two dimensions:

1. Type of attack - either volumetric or application
2. Direction of the attack - either *North-to-South* or *East-to-West*.
 - a. *North-to-South* is an attack that originates outside the ISP's network and targets an ISP customer or infrastructure inside the ISP's network.
 - b. *South-to-North* is an attack that originates inside the ISP's network and targets an external entity or infrastructure inside the ISP's network.
 - c. *East-to-West* represents an attack that originates with a customer and targets another customer

Examples:

1. Customer or ISP infrastructure being hit from the outside - north-to-south
2. Customers with buggy home gateways flooding ISP DNS servers - south-to-north
3. Customers flooding packets to an external target - also south-to-north
4. Customers attacking each other - east-to-west

The sub-group suggested that we separate out customers attacking each other from customers attacking infrastructure or external targets because it sometimes requires different detection and mitigation strategies. For instance, if two customers in the same region attack each other, the traffic might not cross any of the routers from which the ISPs collect flow data, and it would not hit scrubbing centers at the ISP's peering edge.

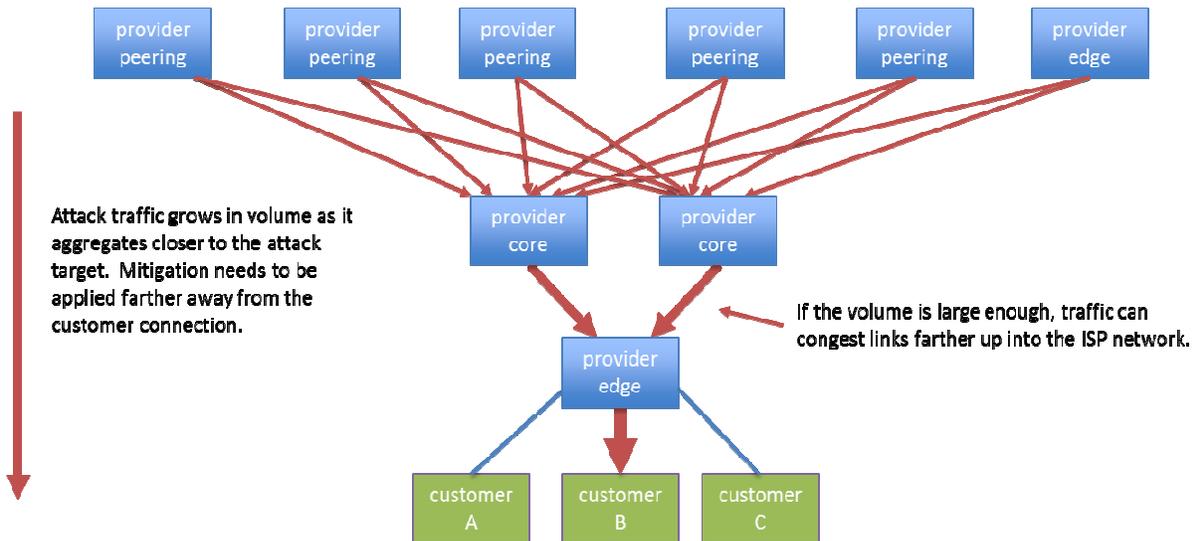
III. Example DDoS Attacks Experienced by ISPs

A. Server-based volumetric DoS attack against a large customer

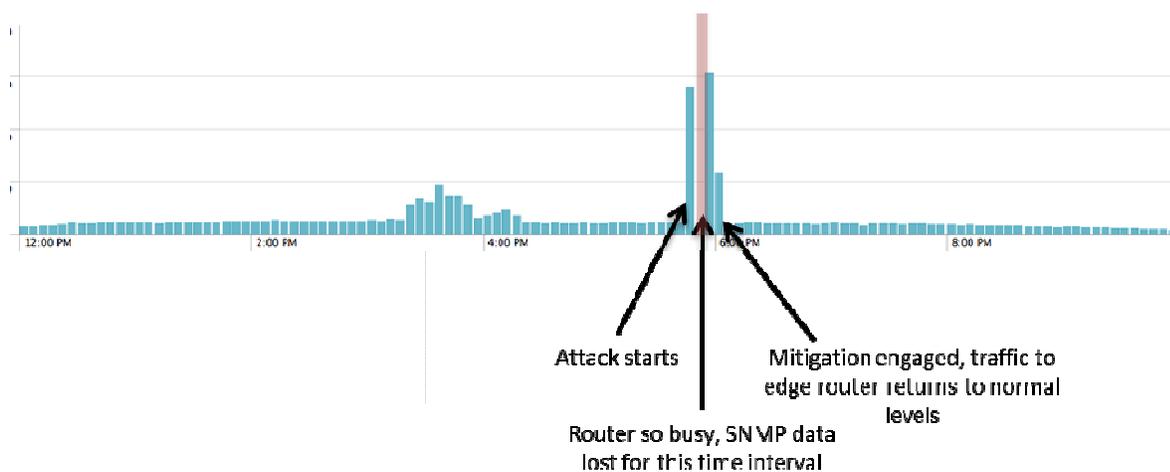
Background: This attack used UDP/80 packets (garbage traffic) in high volume to exhaust the target's bandwidth. The attack took roughly 10 minutes to reach peak volume of over 70Gbps. At the time this was one of the largest attacks seen on the ISP's network. Attacking IPs numbered in the thousands.

Mitigation Steps:

1. The attack was identified along with a target IP by the customer's DoS detection service.
2. The customer engaged the DoS mitigation service, the traffic was re-routed to the DoS mitigation centers. The attack traffic was dropped and legitimate traffic delivered.



With larger attacks (10s to 100s of Gbps), there is a risk of collateral impact to customers not targeted by the attack. Collateral damage can often be avoided if the attack is detected and mitigated quickly.



Recommended Practices:

1. Blackhole routing should be configured on ISP routers in case a customer is attacked that does not subscribe to any DoS mitigation service.
2. Network instrumentation and alarming based on SNMP polling, netflow, probes, or a similar technology is critical to detecting bandwidth saturation problems quickly (15 minutes or less).
3. Netflow collection or some similar technology should be deployed to identify attack targets and target protocols.
4. Providers offering attack mitigation/scrubbing services should engineer the infrastructure

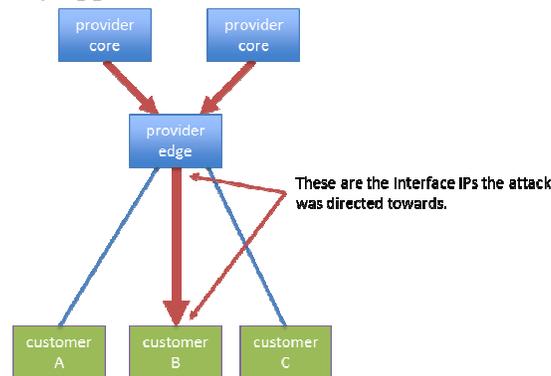
such that attack traffic isn't concentrated in a single area or scrubbing center. Capacity to those centers should be sized appropriately.

B. Attack Directed at ISP and Customer Infrastructure IPs

Background: This attack again used UDP/80 packets (garbage traffic) in high volume to exhaust the target's bandwidth. However, in this case the attack was directed first at the customer's router interface IP and then at the ISP's.

Mitigation Steps:

1. The attack was identified along with a target IP via netflow.
2. The /30 subnet between the ISP and the customer was blackholed.
3. Filters were subsequently applied on ISP border routers to limit traffic destined for ISP infrastructure.



Recommended Practices:

- Limit traffic to ISP point-to-point infrastructure as much as practical, whether by filtering or routing.
- Do not use point-to-point infrastructure IPs for NAT, termination of tunnels, or other traffic that requires IPs to be advertised and routed when they would otherwise not need to be.
- Implement detection as suggested in Case Study 1 so these attacks can be identified quickly. Note that when an ISP address is the target of the attack, the customer will never see the traffic.

Potential Challenges:

- Filtering at every ISP ingress point may be impractical.
- Re-addressing a network to space that is not routed may be a difficult, time-consuming task.

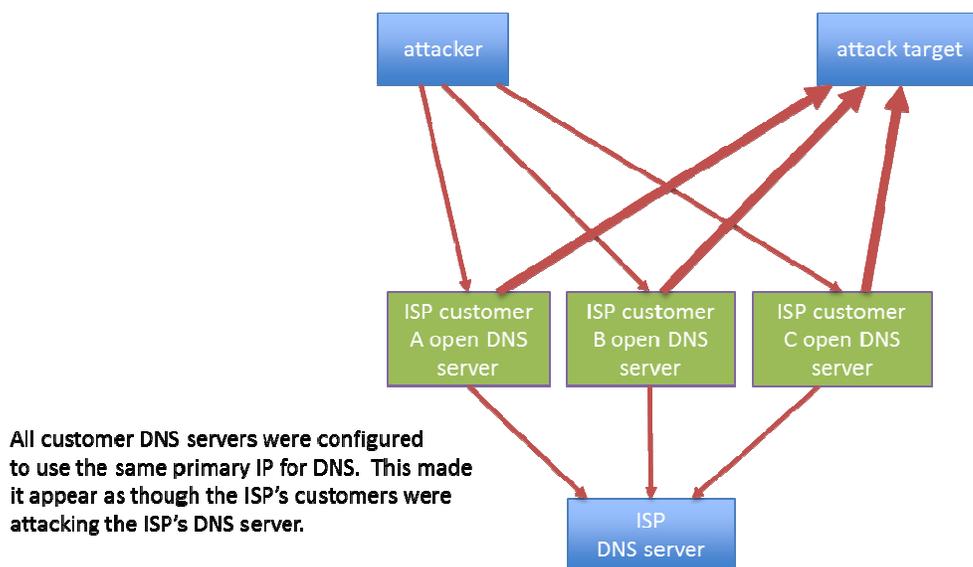
C. Collateral Damage from DNS Reflection Attack

Background: This attack again used spoofed UDP/53 packets (DNS queries) in high volume towards unfiltered recursive DNS servers to magnify the attack and exhaust the target's bandwidth. In this case, the ISP was at risk for adverse impact even though the attack wasn't directed at the ISP at all.

Mitigation Steps:

1. The attack was identified along with a target IP via netflow as well as logging configured on the DNS server.
2. Queries from customers were routed through a DoS mitigation service.

3. ISP later followed up to get customer equipment properly filtered.



Recommended Practices:

- Configure attack mitigation services for critical infrastructure like DNS services. Examples of mitigation include traffic scrubbing and service rate-limiting.
- Expand mitigation capacity as needed for infrastructure services.
- Distribute critical services using technologies like anycast or content distribution networks when possible.
- Provision out-of-band management for critical infrastructure such that an attack does not impede access to equipment needed to mitigate the attack.
- Limit the exposure of services to only those that need access to them (eg DNS, NTP, etc).
- Avoid use of equipment configured with unprotected services such as unfiltered DNS and known SNMP community strings.
- Apply anti-spoofing controls where practical and possible, for example residential networks and hosting centers.

Potential Challenges:

- Provisioning mitigation capacity can be an “arms race” with attackers.
- Some services cannot be effectively filtered without unacceptable collateral impact.
- Anti-spoofing (BCP 38) is not possible for many transit customers.

D. Home Gateway/Router Originated DDoS

- **Background:** A particular home gateway vendor had a bug that causes it to flood DNS requests at line rate when the modem in front of it reboots. The ISP increased broadband speeds in their largest market, requiring modem reboots. Approximately 250 home gateways began flooding DNS requests, taking down the ISP's DNS cluster
-
- **Problems Discovered:**
- No DDOS mitigation capability that deep into the ISP's network. Data scrubbing centers sit at the peering edge of the ISP's network.

- DNS servers were returning additional, optional authority information with each reply, causing an amplification effect
- Rate limiting features were not used at the ISP's load balancers
- ISP had difficulty managing the DNS servers through the query interfaces, which were saturated due to the broadband modem DNS flooding.

- **Mitigation Steps:**

1. Used out of band security tools that capture DNS packets. Configured the tools to count the number of packets seen over a given time period and generate alerts on customers exceeding those thresholds.
2. Fed the alerts into the existing abuse management system and took the customers offline
3. Automated the process for future use

- **Recommendations:**

- For any given service, make sure it returns as little information as possible so it can't be readily used as an amplifier.
- Ensure servers remain reachable when under attack by separating management interfaces from service interfaces.
- Employ the security features (such as rate limiting) available in existing networking hardware.
- Mitigation can be accomplished out of line using passive monitors that signal other tools to take some action.

E. Null Routing

Background: Null routing is the simplest form of DDOS mitigation, but also the one with the most collateral damage. It's a hammer dropping all traffic destined for a given IP address.

Pros:

- Simple and quick to implement
- Drops traffic at the peering edge of the network on the largest links

Cons:

- Drops all traffic to a given IP and not just the malicious traffic

Use cases:

- Residential (or other dynamic IP) customer under attack. The ISP can simply drop all traffic destined for the target IP and give the customer a new one
- Outbound attack. If an IP address at another ISP is under attack, and that ISP indicates there's no legitimate need for our customers to reach it, the first ISP can drop the packets before they leave its network. Example: another ISP's router is under attack. The first ISP's customers have no reason to send packets directly to that router, so they null route its ip on our network.

IV. ISP Mitigation Techniques (Tools/Technical Controls)

There are two primary phases to responding to DDoS attacks:

Phase 1: Detection

DDoS attacks can be detected by ISPs using either volumetric or application based methods. For example, in the case of volumetric based solutions ISPs would establish baseline against which attack traffic anomalies can be determined. Another means to detect attacks is directly from customers who also often observe gradual increases in ingress traffic volumes on their own, and will contact ISPs accordingly.

Detection:

Type	North-to-South	South-to-North	East-to-West
Volumetric	<ul style="list-style-type: none"> • Netflow-based solutions • Utilization monitoring • Call from victim 	<ul style="list-style-type: none"> • Netflow-based solutions • Call from victim 	<ul style="list-style-type: none"> • Call from victim
Application ¹¹	<ul style="list-style-type: none"> • DPI-based solutions • Host-based solutions • Call from victim 	<ul style="list-style-type: none"> • DPI-based solutions • Host-based solutions • Call from victim 	<ul style="list-style-type: none"> • Call from victim

Phase 2: Mitigation

The mitigation phase of DDOS response activity has the goal of countering the effects of the malicious action. Mitigation typically takes the form of either (1) filtering bad traffic, or (2) reducing the intensity of the attack by degrading the botnet source. This second action can be done in variety of ways such as contacting the owners of infected PCs and servers before, during, and after an attack. Thus, the primary goal of ISPs DDOS security activities involves all possible attempts to successfully block, divert, filter, and slow down attack traffic embedded in the normal stream of ingress traffic aimed at a victim site. Since most DDOS attacks vary widely (in contrast to the recent banking attacks, which followed a more routine cadence), the decision process can be highly dynamic, and is usually dependent on real-time analysis.

Mitigation:

Generally speaking, the simplest mitigation technique that will solve the problem is often preferred. From a service perspective, however, more specific mitigation techniques are preferred over those that are more blunt and have greater impact on legitimate traffic. As noted previously, the appropriate action in a given situation does depend on the specifics of the attack and the target.

Blackhole routes are the preferred mitigation in the case that the service or customer under attack will not suffer any degradation or outage by losing all traffic to the target. For example,

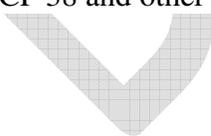
¹¹ Application layer DDOS attacks can be more difficult to detect and in some instances may require more intrusive tools than traditional volumetric based tools such as the use of Deep Packet Inspection (DPI) and can also be complicated by the use of SSL or other based encryption.

in the case that the target address never needs to receive any traffic from the Internet, a blackhole route of that IP is the simplest answer. Additionally, an outbound attack could also be mitigated by blackhole routing the attack target. If services are required of the target address, but the attack is using a different protocol or service, then a packet filter like a router ACL may be effective. Non-trivial volumetric attacks – those targeted at needed services – often require more specialized scrubbing services or DPI solutions. These services are designed to allow most legitimate traffic to pass while blocking most attack traffic.

Type	North-to-South	South-to-North	East-to-West
Volumetric	<ul style="list-style-type: none"> • Scrubbing center/offramp • blackhole route • router ACL • BGP Flowspec 	<ul style="list-style-type: none"> • Suspend attacker’s service • Other device control, such as blocking ports on a modem • blackhole route • router ACL 	<ul style="list-style-type: none"> • Suspend attacker’s service • Other device control, such as blocking ports on a modem • blackhole route • router ACL
Application	<ul style="list-style-type: none"> • Scrubbing center/offramp • DPI-based solutions • Host-based solutions 	<ul style="list-style-type: none"> • DPI-based solutions • Host-based solutions • Suspend attacker’s service • Other device control, such as blocking ports on a modem 	<ul style="list-style-type: none"> • Suspend attacker’s service • Other device control, such as blocking ports on a modem • Host-based solutions

V. Additional Recommendations

- ISPs review the *ABCs for ISPs* set of recommendations for malware mitigation published by CSRIC III in 2012 given that many DDoS attacks have emanated from infected end users.
- Similar best practices be developed for hosting providers in terms of abuse desk and notification processes to alert infected tenants of hosting centers given data center based attacks.
- ISPs review BCP 38 and other alternatives to potentially manage IP address spoofing.



Financial Subgroup Case Study

Case Study:

From late 2012 into mid 2013, US Financial Institutions (USFIs) experienced ongoing Distributed Denial of Service (DDoS) attacks against their networks. Analysis indicates that some of the attacks originate from a nation state threat actor. These attacks show evidence of preplanning and continue to evolve in complexity.

It is believed that the DDoS attacks on the USFIs were part of a larger attack strategy and portend more serious attacks. The USFIs targeted represent a significant component of US economic activity, are emblematic of US economic stability and if compromised could pose a systemic risk to the financial sector. The groups claiming credit have threatened more attacks.

What is a DDOS Attack?

A DDoS attack is a coordinated cyber-attack with the intent to disrupt the availability of an information processing system(s) or application(s) by consuming network bandwidth or by overwhelming the target system with simultaneous data connections from multiple autonomous sources. The distributed model has given rise to botnets, which are collections of malware-infected hosts that have the capability of launching DDoS attacks at the will of the adversary who controls them to significantly change the velocity of attacks.

DDoS Types Used:

- UDP Flooding
- TCP Flooding
- Search function attacks
- Large file GET
- Infrastructure-level attacks
- Authentication portal attacks

Steps in attack:

- Port 80 SYN Flood with some UDP to overwhelm network bandwidth if possible.
- Attack DNS Servers with malformed UDP/TCP packets.
- Attack DNS ports on web servers.
- Attack SSL Connections.
- URLs (latest tactic) switch from main site to secondary sites.
- HTTP/HTTPS Post attacks (Search functions).
- Ports 80/443/53

Tools:

- The attackers use customized attack scripts sending traffic to Ports 80, 443, 53, 1800

Adaptive Techniques:

- Significant volume (Bandwidth/Packets) constant morphing (Port/Protocol).

- On the fly customization of attacks to address mitigation.
- Ability to compromise and then utilize malware-infected servers with high bandwidth connections.
- Ability to add to bots and add new clients to evade IP filters/blacklists.

While the attacks in 2012/13 centered mostly on bandwidth attacks (Layer 3 & 4); the threat actors shifted and evolved their capabilities to conducting more complicated Layer 7 attacks. Using SSL, threat actors engineered attacks so the attacking traffic would seem like legitimate traffic in an attempt to camouflage their nefarious activities and fool network defenses. Further, attacks evolved from single targets, with attackers “dwelling” on a target for hours or days, to attacks against multiple USFIs concurrently or in rapid succession.

Technical Controls:

1. Carrier protocol rate limiting
2. Carrier source IP blocking
3. Carrier blackhole filtering of the destination IP address or protocol
4. Load balancers filtering using custom scripts
5. On-premise web application firewalls
6. Third party BGP-based data scrubbing
7. Third party DNS-based data scrubbing
8. IPS rules
9. Network blocks based on layer 3 or 4 characteristics
10. On-premise DDoS detection/mitigation equipment
11. Carrier blocking based on source IP geography
13. Connection rate limiting
15. On-premise packet/session Time-to-Live (TTL) filtering
16. On-premise protocol/Port filtering

Emerging Trends

- The botnet architecture is becoming more sophisticated and difficult to trace and C2 (Command and Control) systems are increasingly tiered using proxy servers to obfuscate the location of the system that is executing the commands.
- 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.
- Botnets are becoming extremely sophisticated, and some have the ability to wipe a compromised system’s entire hard drive after it has completed an attack.
- DDoS tools are/will continue to become more sophisticated, with multi-tasking and multithreading capabilities that will provide the potential to launch attacks on multiple targets and services simultaneously.
- Social media such as Twitter could potentially be used to redirect and configure zombies as new attack vectors.
- With the proliferation of mobile devices, adversaries will compromise and install botnets and leverage them to conduct DDoS attacks.

- Attackers have developed the ability to actively monitor defensive actions and continuously adapt their attacks to attempt to defeat mitigation. Attackers have demonstrated the capability to add to the bots, adding new clients to evade IP filters/blacklists.

DRAFT

Internet Security Experts Subgroup Case Studies

Case Study #1: Outbound/crossbound DDoS attack launched by servers in an Internet Data Center (IDC)

Servers compromised in an IDC due to vulnerable versions of software; no root, no spoofed traffic.

- Multiple, shifting attack vectors – HTTP, HTTP/S, malformed DNS query floods; GETs via HTTP & HTTP/S consuming outbound transit bandwidth on target networks. Collateral impact to legitimate server users, IDC operators, transit network operators.
- High packets per second (pps) / bits per second (bps) per source

Case Study #2: DNS reflection/amplification attack leveraging open DNS recursors.

The attacker spoofs the IP address of the target of the attack, sending DNS queries for pre-identified large DNS records (ANY records, large TXT records, etc.) either to abusable open DNS recursive servers, or directly to authoritative DNS servers.

The attacker chooses the UDP port which he'd like to target – with DNS, this is typically limited to either UDP/53 or UDP/1024-65535. The destination port is UDP/53

The servers 'reply' either directly to the attack target or to the intermediate open DNS recursive servers with large DNS responses – the attack target will see streams of unsolicited DNS responses broken down into initial and non-initial fragments.

Response sizes are typically 4096 – 8192 bytes (can be smaller or larger), broken down into multiple fragments.

Packet sizes received by the attack target are generally ~1500 bytes due to prevalent Ethernet MTUs – and there are lots of them.

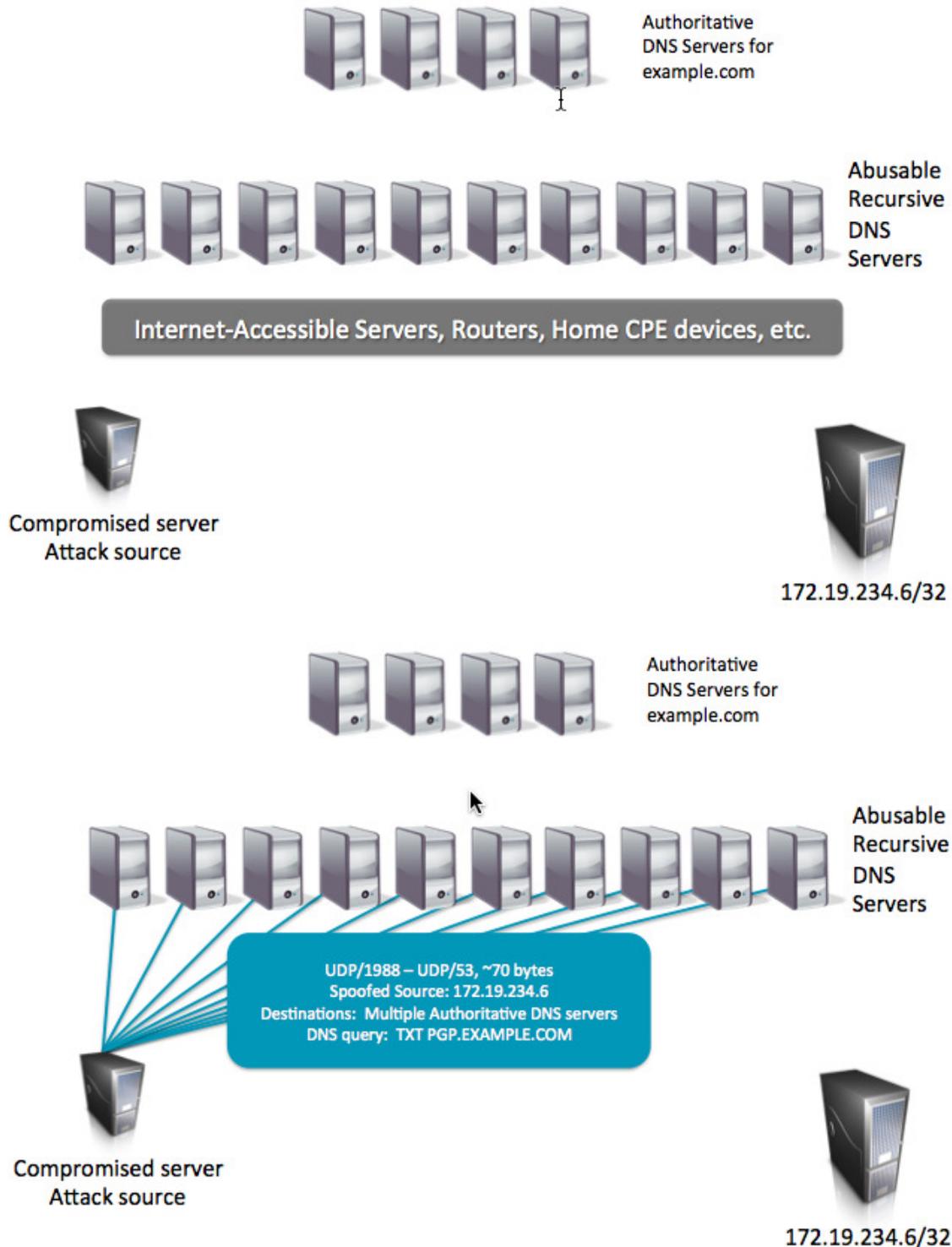
As these multiple streams of fragmented DNS responses converge, the attack volume can be huge – the largest verified attack of this type so far is ~200gb/sec. 100gb/sec attacks are commonplace.

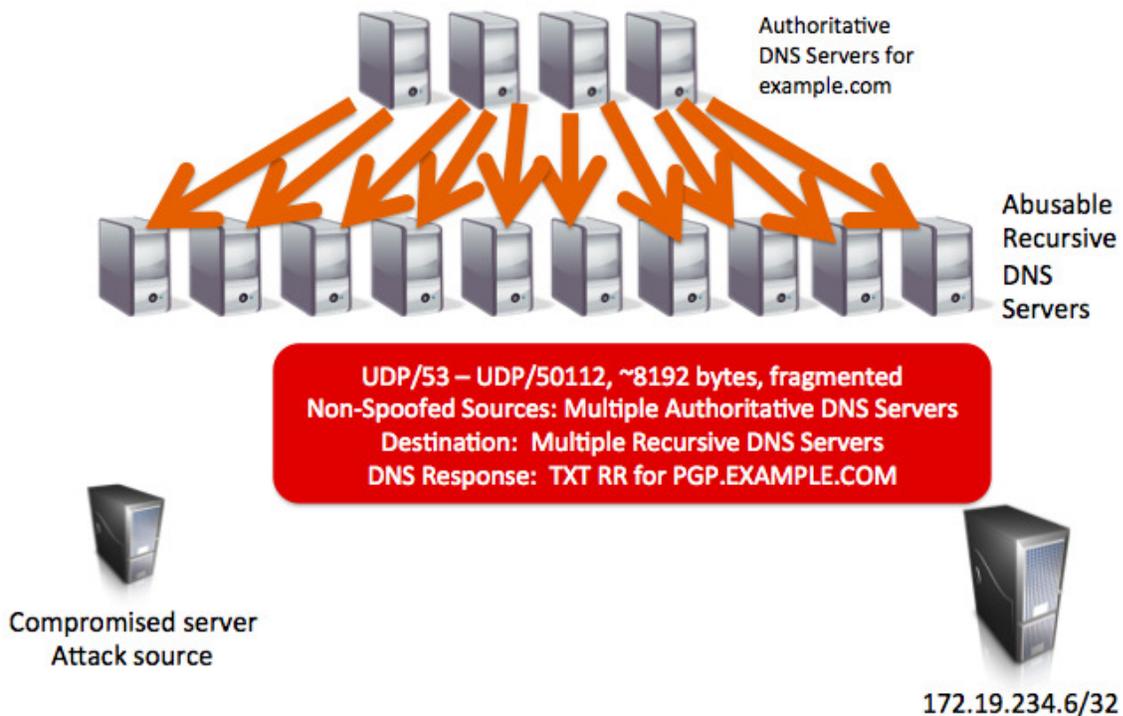
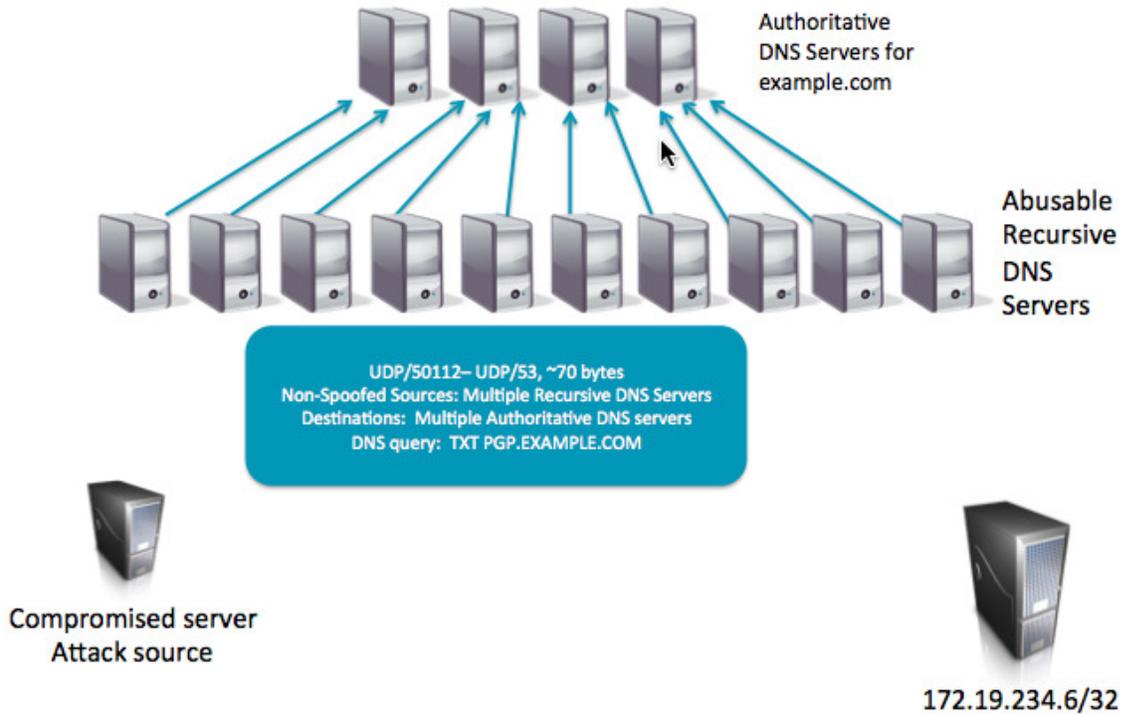
Internet transit bandwidth of the target, along with core bandwidth of the target's peers/upstreams, as well as the core bandwidth of intermediary networks between the various DNS services being abused and the target, are saturated.

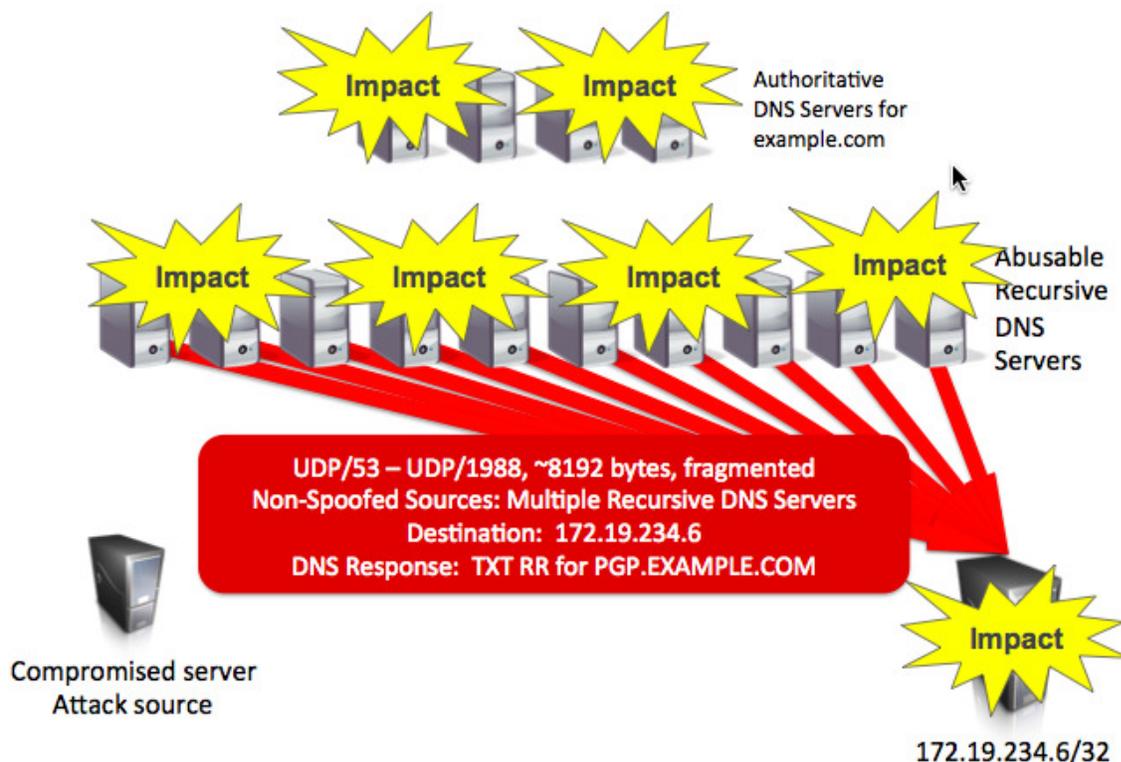
In most attacks involving intermediate open DNS recursive servers are reflectors, between ~20,000 – 30,000 abusable recursive DNS are leveraged by attackers. Up to 50,000 abusable open recursive DNS servers have been observed in some attacks.

In attacks leveraging authoritative DNS servers directly, hundreds or thousands of these servers are utilized by attackers.

Many well-known authoritative DNS servers are anycasted, with multiple instances deployed around the Internet.







Case Study #3: Endpoint enterprise network Web server targeted by ntp reflection/amplification attack.

The attacker spoofs the IP address of the target of the attack, sends monlist, showpeers, or other NTP level-6/-7 administrative queries to multiple abusible NTP services running on servers, routers, home CPE devices, etc.

The attacker chooses the UDP port which he'd like to target – typically, UDP/80 or UDP/123, but it can be any port of the attacker's choice – and uses that as the source port. The destination port is UDP/123.

The NTP services 'reply' to the attack target with non-spoofed streams of ~468-byte packets sourced from UDP/123 to the target; the destination port is the source port the attacker chose when generating the NTP monlist/showpeers/etc. queries.

As these multiple streams of non-spoofed NTP replies converge, the attack volume can be huge – the largest verified attack of this type so far is over 400gb/sec. 100gb/sec attacks are commonplace.

Due to sheer attack volume, the Internet transit bandwidth of the target, along with core bandwidth of the target's peers/upstreams, as well as the core bandwidth of intermediary networks between the various NTP services being abused and the target, is saturated with non-spoofed attack traffic.

In most attacks, between ~4,000 - ~7,000 abusible NTP services are leveraged by attackers. Up to 50,000 NTP services have been observed in some attacks.

Servers, services, applications, Internet access, et. al. on the target network overwhelmed and rendered unavailable by sheer traffic volume – tens or hundreds of gb/sec frequent.

Complete saturation of peering links/transit links of the target network.

Total or near-total saturation of peering links/transit links/core links of intermediate networks between the NTP reflectors/amplifiers and the target network – including the networks of direct peers/transit providers of the target network

Widespread collateral damage – packet loss, delays, high latency for Internet traffic of uninvolved parties which simply happens to traverse networks saturated by these attacks.

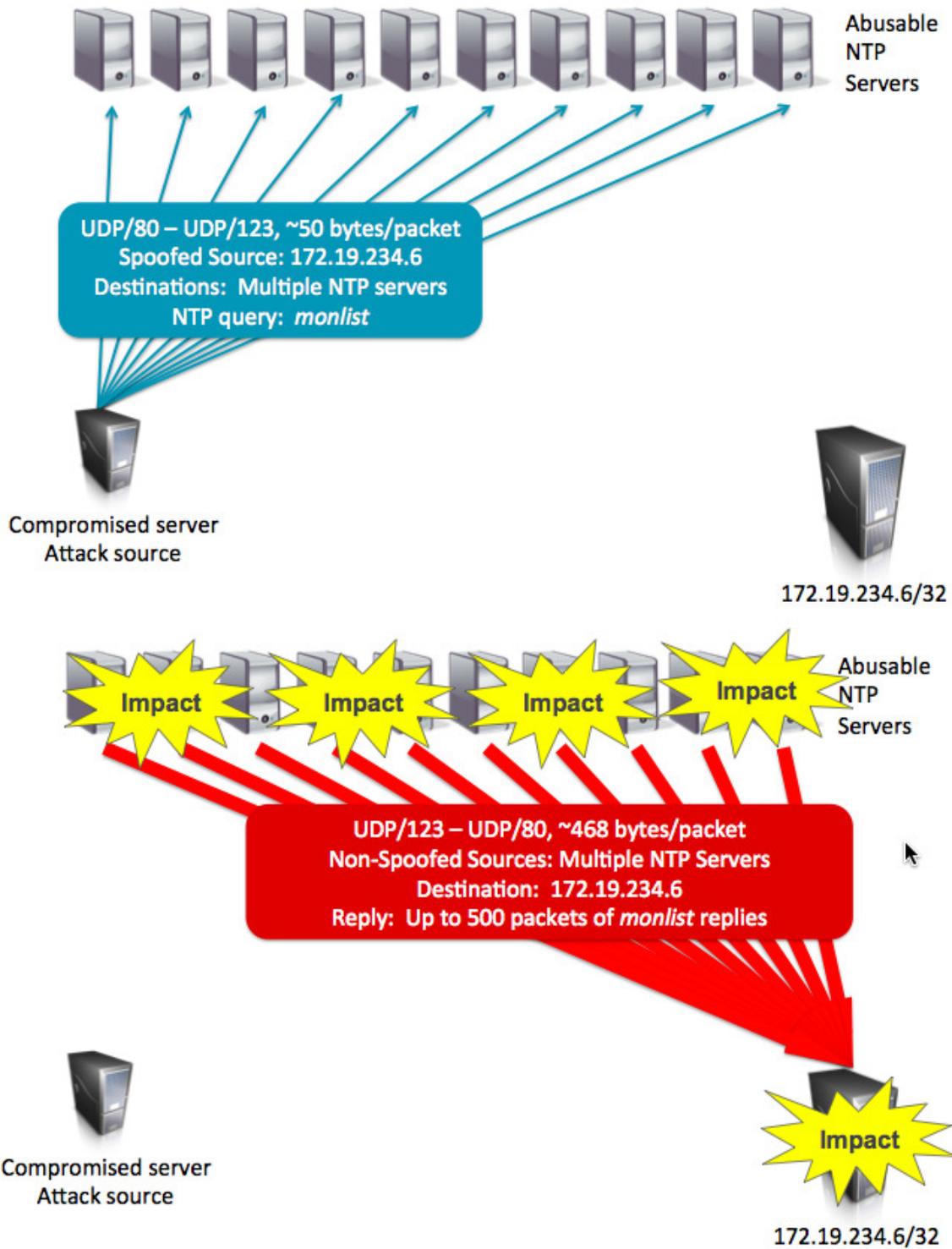
Unavailability of servers/services/applications, Internet access for bystanders topologically proximate to the target network.

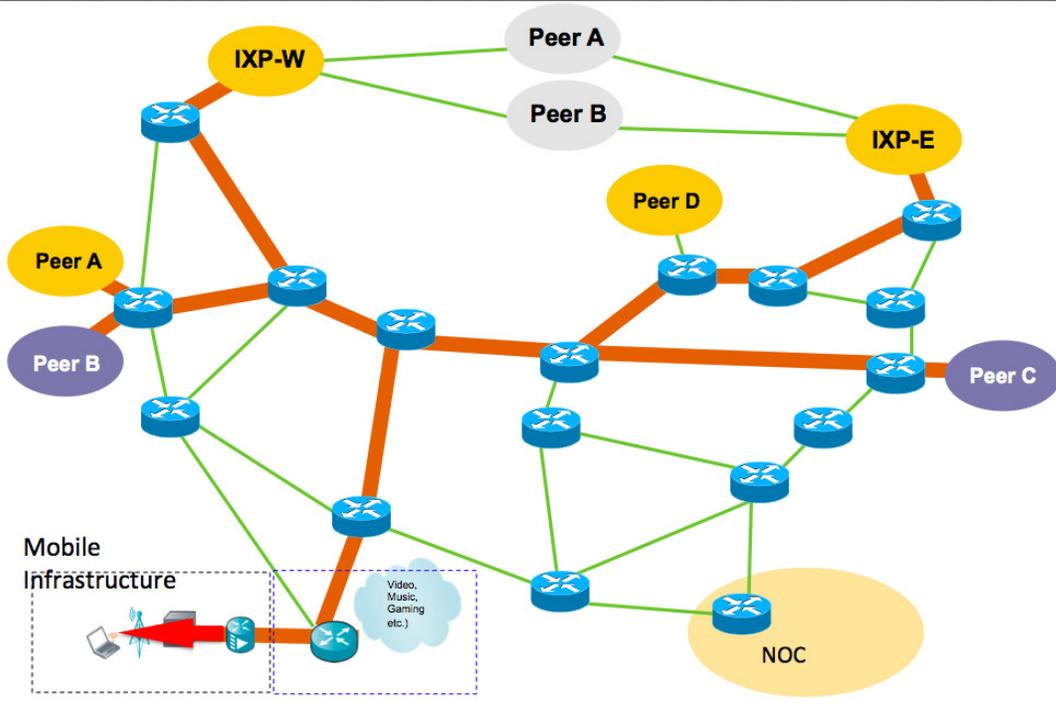
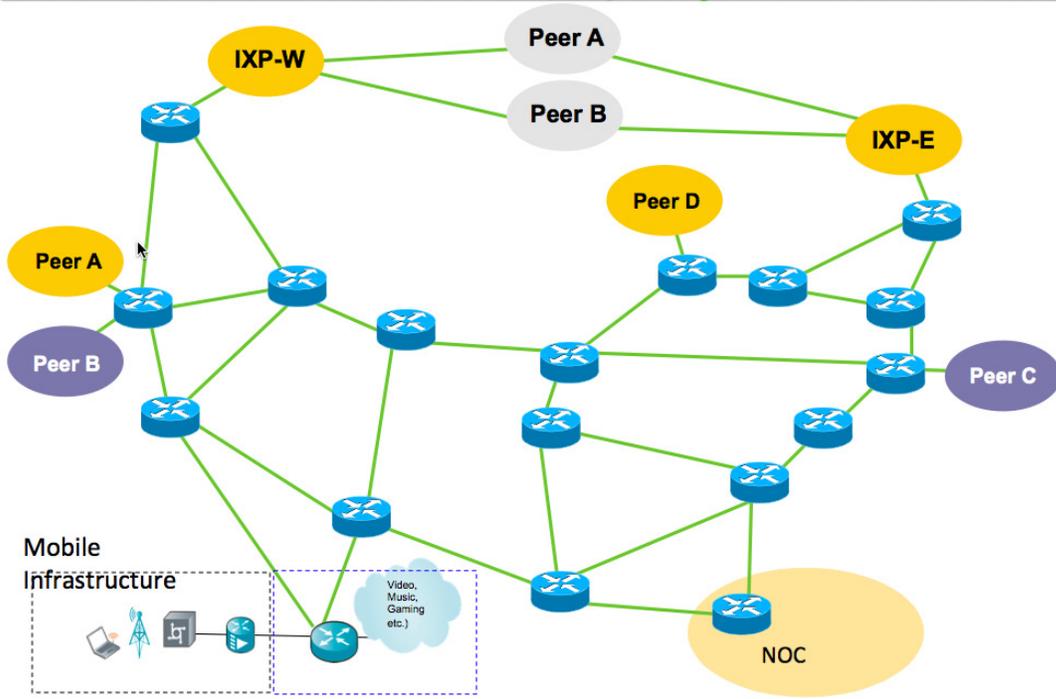


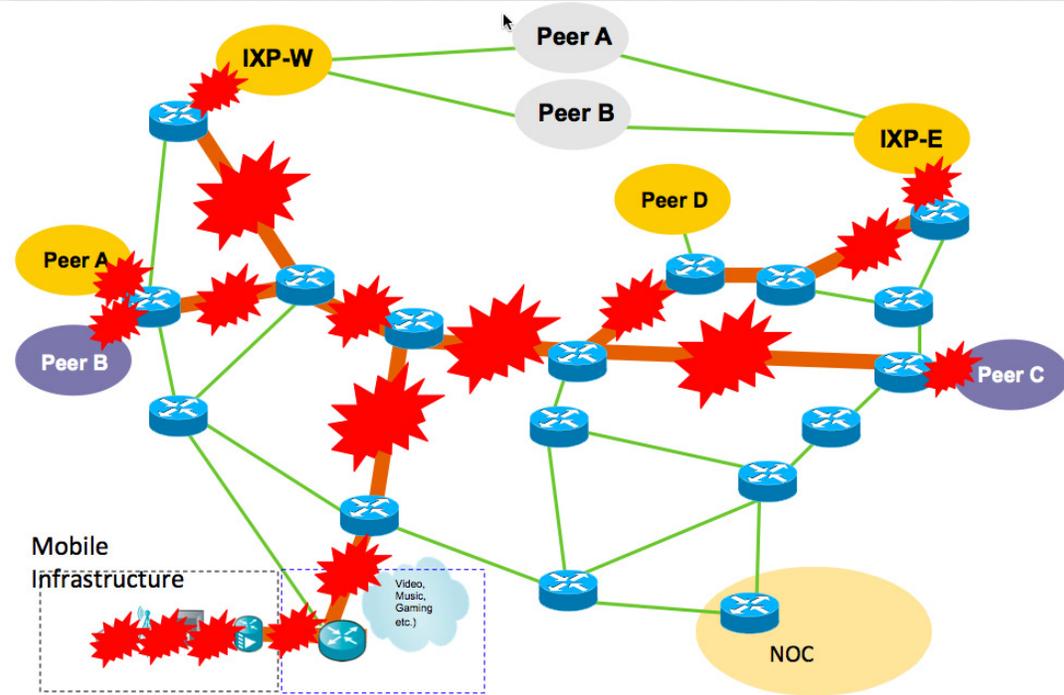
Compromised server
Attack source



172.19.234.6/32







DRAFT

Appendix E: Best Practices

Introduction to Best Practices

Best Practices are statements that describe the industry's guidance to itself for the best approach to addressing a concern. They result from unparalleled industry cooperation that engages vast expertise and considerable resources. The primary objective of Best Practices is to provide guidance from assembled industry expertise and experience. The implementation of Best Practices is intended to be voluntary. Decisions of whether or not to implement a specific Best Practice are intended to be left with the responsible organization (e.g., Service Provider, Network Operator, or Equipment Supplier). In addition, the applicability of each Best Practice for a given circumstance depends on many factors that need to be evaluated by individuals with appropriate experience and expertise in the same area addressed by the Best Practice.

The Best Practices recommended by CSRIC IV Working Group 5 are intended to give guidance. Decisions of whether or not to implement a specific Best Practice are intended to be left with the responsible organization (e.g., Service Provider, Network Operator, or Equipment Supplier). Mandated implementation of these Best Practices is not consistent with their intent. The appropriate application of these Best Practices can only be done by individuals with sufficient knowledge of company specific network infrastructure architecture to understand their implications. Although the Best Practices are written to be easily understood, their meaning is often not apparent to those lacking this prerequisite knowledge and experience. Appropriate application requires understanding of the Best Practice impact on systems, processes, organizations, networks, subscribers, business operations, complex cost issues, and other considerations. With these important considerations regarding intended use, the industry stakeholders are concerned that government authorities may inappropriately impose these as regulations or court orders. Because these Best Practices have been developed as a result of broad industry cooperation that engages vast expertise and considerable voluntary resources, such misuse of these Best Practices may jeopardize the industry's willingness to work together to provide such guidance in the future.¹²

¹² These principles were brought forward from the work of the NRIC VII Focus Group 3B, Public Data Network Reliability Final Report, Sections 2.3.2 and 3.4.2.

WG5 has identified the following Categories for Best Practices to mitigate server-based DDoS attacks:

Preparation

Identification

Classification

Traceback

Reaction

Post Mortem & Recovery

The following Best Practices address server-based DDoS attacks. These best practices will be further refined, prioritized and new recommendations added for the final report.

Existing Best Practices:

BP Number: 9-7-8076

Denial of Service (DoS) Attack:

Vendor: Equipment Suppliers should develop effective DoS/DDoS survivability features for their product lines.

BP Reference/Comments:

e.g., SYN Flood attack defense, CERT/CC ® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks - <http://www.cert.org/advisories/CA-1996-21.html>. Related to NRIC BP 8563.

BP Number: 9-8-0507:

Attack Trace Back:

Service Providers, Network Operators and Equipment Suppliers should have the processes and/or capabilities to analyze and determine the source of malicious traffic, and then to trace-back and drop the packets at, or closer to, the source. The references provide several different possible techniques. (Malicious traffic is that traffic such as Distributed Denial of Service (DDoS) attacks, smurf and fraggle attacks, designed and transmitted for the purpose of consuming resources of a destination of network to block service or consume resources to overflow state that might cause system crashes).

BP Reference/Comments:

"Practical Network Support for IP Trace back" by Stefan Savage et.al., Dept. of Computer Science and Engineering, Univ of Washington, Tech Report UW-CSE-2000-02-01 with a version published in the Proceedings of the 2000 ACM SIBCOMM pp256-306 Stockholm, Sweden, August 2000

BP Number: 9-8-0806

Service Policies:

Service Providers should establish policies and develop internal controls to ensure that the infrastructure supporting high speed broadband is protected from external threats, insider threats and threats from customers. These policies should cover protocol and port filtering as well as general security best practices.

BP Reference/Comments:

None.

BP Number: 9-8-8096

Users Should Employ Protective Measures:

Service Providers and Network Operators should educate service customers on the importance of, and the methods for, installing and using a suite of protective measures (e.g., strong passwords, anti-virus software, firewalls, IDS, encryption) and update as available.

BP Reference/Comments:

<http://www.stonybrook.edu/nyssecure>, <http://www.fedcirc.gov/homeusers/HomeComputerSecurity/>
Industry standard tools (e.g., LC4).

BP Number: 9-8-8514

Recovery from Network Misuse via Invalid Source Addresses:

Upon discovering the misuse or unauthorized use of the network, Service Providers should shut down the port in accordance with AUP (Acceptable Use Policy) and clearance from legal counsel. Review ACL (Access Control List) and temporarily remove offending address pending legal review and reactivate the port after the threat has been mitigated.

BP Reference/Comments:

IETF rfc3013 sections 4.3 and 4.4. NANOG ISP Resources. www.IATF.net.

BP Number: 9-8-8913

Maintain Methods to Detect Bot/Malware Infection:

ISPs should maintain methods to detect likely malware infection of customer equipment. Detection methods will vary widely due to a range of factors. Detection methods, tools, and processes may include but are not limited to: external feedback, observation of network conditions and traffic such as bandwidth and/or traffic pattern analysis, signatures, behavior techniques, and forensic monitoring of customers on a more detailed level.

BP Reference/Comments:

More information can be found at:

<http://teamcymru.org>

<http://shadowserver.org>

<http://abuse.ch>

<http://cbl.abuseat.org>

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

BP Number: 9-8-8914

Use Tiered Bot Detection Approach:

ISPs should use a tiered approach to botnet detection that first applies behavioral characteristics of user traffic (cast a wide net), and then applies more granular techniques (e.g., signature detection) to traffic flagged as a potential problem.

BP Reference/Comments:

This technique should help minimize the exposure of customer information in detecting bots by not collecting detailed information until it is reasonable to believe the customer is infected. Looking at user traffic using a wide net approach can include external feedback as well as other internal approaches.

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

BP Number: 9-9-8065

Network Operators, Service Providers, Public Safety and Equipment Suppliers should establish a process for releasing information to members of the law enforcement and intelligence communities and identify a single Point of Contact (POC) for coordination/referral activities.

BP Reference/Comments:

None.

BP Number: 9-9-8068

Service Providers, Network Operators, Public Safety, and Equipment Suppliers should develop and practice a communications plan as part of the broader Incident response plan identifying key players to include as many of the following items as appropriate: contact names, business telephone numbers, home telephone numbers, pager numbers, fax numbers, cell phone numbers, home addresses, internet addresses, permanent bridge numbers, etc. Notification plans should be developed prior to an event/incident happening where necessary. The plan should also include alternate communications channels (e.g., alpha pagers, internet, satellite phones, VOIP, private lines, smart phones) balancing the value of any alternate method against the security and information loss risks introduced.

BP Reference/Comments:

Alternate broadband communication path for coordination and management.

DRAFT

Updated Best Practices (Work In Progress):

BP Number: 9-7-0408

Ingress Filtering:

Network Operators and Service Providers should, where feasible, implement RFC 3704 (IETF BCP84) ingress filtering.

BP Reference/Comments:

See <http://www.IETF.org>

WG5 Note: Update to add higher level anti-spoofing BP with implementation guidance split into single-homed and multi-homed environments.

BP Number: 9-8-8047

Protect Against DNS (Domain Name System) Denial of Service:

Service Providers and Network Operators should provide DNS DoS protection by implementing protection techniques such as: 1) increase DNS resiliency through redundancy and robust network connections, 2) Have separate name servers for internal and external traffic as well as critical infrastructure, such as OAM&P and signaling/control networks, 3) Where feasible, separate proxy servers from authoritative name servers, 4) Protect DNS information by protecting master name servers with appropriately configured firewall/filtering rules, implement secondary masters for all name resolution, and using Bind ACLs to filter zone transfer requests.

BP Reference/Comments:

RFC-2870, ISO/IEC 15408, ISO 17799, US-CERT "Securing an Internet Name Server" (<http://www.cert.org/archive/pdf/dns.pdf>).

WG5 Note: Update to combine with 9-8-8118.

BP Number: 9-8-8118

Protect Against DNS (Domain Name System) Distributed Denial of Service:

Service Providers and Network Operators should provide DNS DDoS protection by implementing protection techniques such as: 1) Rate limiting DNS network connections 2) Provide robust DNS capacity in excess of maximum network connection traffic 3) Have traffic anomaly detection and response capability 4) Provide secondary DNS for back-up 5) Deploy Intrusion Prevention System in front of DNS.

BP Reference/Comments:

RFC-2870, ISO/IEC 15408, ISO 17799, US-CERT "Securing an Internet Name Server" (<http://www.cert.org/archive/pdf/dns.pdf>).

WG5 Note: Update to combine with BP 9-8-8047.

BP Number: 9-8-8515

Update to:

Recovery from Misuse or Undue Consumption of System Resources:

If a misuse or unauthorized use of a system is detected, Service Providers and Network Operators should perform forensic analysis on the system, *where practical*, conduct a post-mortem analysis and enforce system resource quotas.

BP Reference/Comments:

IETF RFC2350, CMU/SEI-98-HB-001.

WG5 Note: Update comments to indicate this addresses hosting provider being part of attack as opposed to a victim. Addresses both network and hosts. BP addresses devices that are participating in an attack, e.g., An NTP servers on an ISP network could be used as a reflective device.

BP Number: 9-8-8528

Recover from DNS (Domain Name Server) Denial of Service Attack:

If the DNS server is under attack, Service Providers and Network Operators should consider one or more of the following steps 1) Implement reactive filtering to discard identified attack traffic, if possible, 2) Rate-limiting traffic to the DNS server complex, 3) Deploy suitable Intrusion Prevention System in front of DNS servers, 4) Deploy additional DNS server capacity in a round-robin architecture, 5) Utilize DoS/DDoS tracking methods to identify the source(s) of the attack, or 6) Move name resolution service to a 3rd party provider.

BP Reference/Comments:

RFC-2870, ISO/IEC 15408, ISO 17799 US-CERT "Securing an Internet Name Server".

WG5 Note: Needs rewording. Compare with other DNS BPs that are in scope. May want to modify BP to change "recover" to "mitigate"

BP Number: 9-8-8561

Recovery from Denial of Service Attack - Target:

If a network element or server is under DoS attack, Service Providers and Network Operators should evaluate the network and ensure issue is not related to a configuration/hardware issue. Determine direction of traffic and work with distant end to stop inbound traffic. Consider adding more local capacity (bandwidth or servers) to the attacked service. Where available, deploy DoS/DDoS specific mitigation devices and/or use anti-DoS capabilities in local hardware. Coordinate with HW vendors for guidance on optimal device configuration. Where possible, capture hostile code and make available to organizations such as US-CERT and NCS/NCC for review.

BP Reference/Comments:

WG5 Note: Change "recover" to "mitigate."

BP Number: 9-8-8563

Updated to:

Denial of Service Attack Prevention:

When a denial of service vulnerability or exploit is discovered, ISPs, network operators, hosting providers and hardware/software vendors should work with clients to ensure equipment is updated to remediate the vulnerability. If short term remediation is not possible, equipment or network mitigations should be considered to minimize the likelihood of DDoS attack exploitation. Where possible, analyze hostile traffic for product improvement or mitigation/response options, disseminate results of analysis.

BP Reference/Comments:

None.

BP Number: 9-8-8698

Firewall Protection:

Service Providers & Network Operators should utilize firewall protection on all computing devices.: Whenever available for a mobile communications device, firewall software should be installed and utilized.

BP Reference/Comments:

WG5 Note: Reword to include data center/hosting servers.

BP Number: 9-8-8753

Updated to:

Vulnerability Management:

Service Providers and Network Operators should ensure they can manage security vulnerabilities in products they deploy to customers. Such management may be passive, such as simply maintaining a list of customers to whom they have distributed the product, or - when technically and legally feasible - it may be active, such as vulnerability scanning. Also, products, i.e., equipment/software, should be tested for vulnerabilities prior to deployment.

BP Reference/Comments:

Sans Institute, "Vulnerability Management: Tools, Challenges and Best Practices." 2003. Pg. 12 - 13.

BP Number: 9-8-8901

Update to:

Hosting Providers Support for Educational Resources for Computer Hygiene / Safe Computing:

Hosting Providers should provide or support third-party tutorial, educational, and self-help resources for their customers to educate them on the importance of and help them practice safe computing. Hosting Provider customers should know to protect end user devices and networks from unauthorized access through various methods, including, but not limited to:

- Use legitimate security software that protects against viruses and spywares;
- Ensure that any software downloads or purchases are from a legitimate source;
- Use firewalls;
- Configure computer to download critical updates to both the operating system and installed applications automatically;
- Scan computer regularly for spyware and other potentially unwanted software;
- Keep all applications, application plug-ins, and operating system software current and updated and use their security features;
- Use strong passwords;
- Never share passwords.

BP Reference/Comments:

More information can be found at:

National Cyber Security Alliance - <http://www.staysafeonline.org/>

OnGuard Online - <http://www.onguardonline.gov/default.aspx>

Department of Homeland Security -

StopBadware – http://www.stopbadware.org/home/badware_prevent

Comcast.net Security - <http://security.comcast.net/>

Verizon Safety & Security -

http://www.verizon.net/central/vzc.portal?_nfpb=X&_pageLabel=vzc_help_safety

Qwest Incredible Internet Security site: <http://www.incredibleinternet.com/>

Microsoft- <http://www.microsoft.com/security/pypc.aspx>

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

BP Number: 9-8-8903

Protect DNS Servers:

ISPs should protect their DNS servers from DNS spoofing attacks and take steps to ensure that compromised customer systems cannot emit spoofed traffic (and thereby participate in DNS amplification attacks). Defensive measures include:

- (a) managing DNS traffic consistent with industry accepted procedures;
- (b) where feasible, limiting access to recursive DNS resolvers to authorized users;
- (c) blocking spoofed DNS query traffic at the border of their networks, and
- (d) routinely validating the technical configuration of DNS servers by, for example, utilizing available testing tools that verify proper DNS server technical configuration.

BP Reference/Comments:

Widely accepted DNS traffic management procedures are discussed in the following document:
http://www.maawg.org/sites/maawg/files/news/MAAWG_DNS%20Port%2053V1.0_2010-06.pdf

Security issues on recursive resolvers are discussed in IETF BCP 140/ RFC 5358. Responses to spoofed traffic, including spoofed DNS traffic, are discussed in IETF BCP 38/RFC 2827.

Some tools examining different aspects of DNS server security include:

<http://dnscheck.iis.se/>, <http://recursive.iana.org/>, and

<https://www.dnsoarc.net/oarc/services/dnsentropy>. More information on DNS security issues can also be found at: <http://www.iana.org/reports/2008/cross-pollination-faq.html>

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

WG5 Note: Combine with 9-8-8047

BP Number: 9-8-8912

Communicate Implementation of Situational Awareness and Protective Measures with Other ISPs:

ISPs should make reasonable efforts to communicate with other operators and security software providers, by sending and/or receiving abuse reports via manual or automated methods. These efforts could include information such as implementation of "protective measures" such as reporting abuse (e.g., spam) via feedback loops (FBLs) using standard message formats such as Abuse Reporting Format (ARF). Where feasible, ISPs should engage in efforts with other industry participants and other members of the internet ecosystem toward the goal of implementing more robust, standardized information sharing in the area of botnet detection between private sector providers.

BP Reference/Comments:

See the following document for more information:

<http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf>

Vulnerabilities can be reported in a standardized fashion using information provided at

<http://nvd.nist.gov/>

<http://puck.nether.net/mailman/listinfo/nsp-security>

<https://ops-trust.net/>

<https://www2.icsalabs.com/veris/>

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

WG5 Note: Reword to more broadly address concept of ISP collaboration, e.g., STIX and TAXII.

BP Number: 9-8-8916

Updated to:

Bot Detection and the Corresponding Notification Should Be Timely:

ISPs and Hosting Providers should ensure that bot detection and the corresponding notification to hosting customers be timely, since such security problems are time-sensitive. If complex analysis is required and multiple confirmations are needed to confirm a bot is indeed present, then it is possible that the malware may cause some damage, to either the infected host or remotely targeted system (beyond the damage of the initial infection) before it can be stopped. Thus, an ISP or Hosting Provider must balance a desire to definitively confirm a malware infection, which may take an extended period of time, with the ability to predict the strong likelihood of a malware infection in a very short period of time. This 'definitive-vs.-likely' challenge is difficult and, when in doubt, ISPs and Hosting Providers should error on the side of caution by communicating a likely malware infection while taking reasonable steps to avoid false positive notifications.

BP Reference/Comments:

The ISP notification implementation needs to balance the certainty of a detected infection with the uncertainty of a transient detection of malicious traffic to minimize the possibility of false-positive notifications which could become an annoyance to customers and become unmanageable by the ISP.

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide service to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

BP Number: 9-8-8917

Notification to End Users:

ISPs should develop and maintain critical notification methods to communicate with their customers that their computer and/or network has likely been infected with malware. This should include a range of options in order to accommodate a diverse group of customers and network technologies. Once an ISP has detected a likely end user security problem, steps should be undertaken to inform the Internet user that they may have a security problem. An ISP should decide the most appropriate method or methods for providing notification to their customers or internet users, and should use additional methods if the chosen method is not effective. The range of notification options may vary by the severity and/or criticality of the problem. Examples of different notification methods may include but are not limited to: email, telephone call, postal mail, instant messaging (IM), short messaging service (SMS), and web browser notification.

BP Reference/Comments:

An ISP decision on the most appropriate method or methods for providing notification to one or more of their customers or Internet users depends upon a range of factors, from the technical capabilities of the ISP, to the technical attributes of the ISP's network, cost considerations, available server resources, available organizational resources, the number of likely infected hosts detected at any given time, and the severity of any possible threats, among many other factors. The use of multiple simultaneous notification methods is reasonable for an ISP but may be difficult for a fake anti-virus purveyor. Best Practice 8-8-X022 provides information on how to address the malware infection.

Note that the Best Practices in this grouping are primarily aimed at ISPs that provide services to consumer end-users on residential broadband networks, but may be applicable to other users and networks as well.

WG5 Note: May need to combine with 9-8-8916.

BP Number: 8-9-8074

Denial of Service (DoS) Attack - Target:

Where possible, Service Provider and Network Operator networks and Equipment Supplier equipment should be designed to survive significant increases in both packet count and bandwidth utilization. Infrastructure supporting mission critical services should be designed for significant increases in traffic volume and must include network devices capable of filtering and/or rate limiting traffic. Network engineers must understand the capabilities of the devices and how to employ them to maximum effect. Wherever practical, mission critical systems should be deployed in clustered configuration allowing for load balancing of excess traffic and protected by a purpose built DoS/DDoS protection device. Operators of critical infrastructure should deploy DoS survivable hardware and software whenever possible.

BP Reference/Comments:

Note: This Best practice could impact 9-1-1 operations.

Updated to add:

Note that Service Providers, Network Operators, and Equipment Suppliers need to determine which systems are mission critical in the implementation of this best practice.

BP Number: 9-9-8725

Updated to:

Signaling DoS Protection:

Network Operators should establish alarming thresholds for various traffic indicators to ensure that DoS conditions are recognized. Examples include comparison of baselines of normal traffic levels at key network points to current traffic levels, and comparison of baseline of netflow information for both traffic levels and protocols to current traffic levels.

BP Reference/Comments:

Note: This Best practice could impact 9-1-1 operations.

Updated to add: Alarming thresholds are intended to recognize DoS conditions that may a threat to the operator infrastructure.

BP Number: 9-9-8762

Recover from DoS Attack:

Updated to:

Network Operators and Service Providers should when feasible, cooperate with other organizations during and after significant cyber incidents to share information on steps taken to characterize the attack, on techniques to identify, filter, and isolate the originating points of the attack, and on actions taken to reroute legitimate traffic and to deter or defend against similar DoS attacks.

BP Reference/Comments:

IETF RFC2350, CMU/SEI-98-HB-001. Note: This Best practice could impact 9-1-1 operations.

Updated to add:

This best practice is aimed at the recovery of the operator's infrastructure from DoS attack.

New Best Practices (Work In Progress):

BP Number: New BP 1

Application Based Network Firewall Protection:

Hosting Providers should consider application based network and/or host based firewalls, configured to deny traffic by default, to protect against malicious or otherwise unauthorized incoming or outbound network traffic in their hosting centers or on servers.

BP Reference/Comments:

GB973 Guide - 4 /DSD 2011 #8 (Modified)

GB973 Guide - 5 /DSD 2011 #9 (Modified)

BP Number: New BP2

Destination based Black Hole Filtering / Remote triggered Black Hole Filtering:

TBD

BP Reference/Comments:

RFC 4778

BP Number: New BP3

Sinkhole Routing:

TBD

BP Reference/Comments:

RFC 4778

BP Number: New BP4

Source based Black Hole Filtering:

TBD

BP Reference/Comments:

Greene, Barry Raveendran. "Phase 1 – Prepare the Tools and Techniques, Using IP Routing as a Security Tool." ISP Security Bootcamp Singapore 2003. 31 July 2003 <<ftp://ftp-eng.cisco.com/cons/isp/security/ISP-Security-Bootcamp-Singapore-2003/H-Preparation-Tools-v3-0.pdf>>

BP Number: New BP5

Deploy BGP Flowspec:

TBD

BP Reference/Comments:

RFC 5575

BP Number: New BP6

Deploy Anycast for DNS infrastructure:

TBD

BP Reference/Comments:

A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment

BP Number: New BP7

Provide Recursive Name Lookup Service to only the Intended Clients:

TBD

BP Reference/Comments:

IETF BCP 140

BP Number: New BP8

Use Netflow data analysis to detect spoofing attacks:

TBD

BP Reference/Comments:

TBD

BP Number: New BP9

Dropped.

BP Reference/Comments:

None.

BP Number: New BP10

Web service should limit downstream payloads which may result in downstream Dos attacks:

TBD

BP Reference/Comments:

TBD

BP Number: New BP11

Deploy Hosting (IDC) Anti-Spoofing Technology:

TBD

BP Reference/Comments:

TBD

BP Number: New BP12

Prioritization of traffic to ensure critical traffic, e.g., control plane, not affected by server-based DDOS attack:

TBD

BP Reference/Comments:

TBD

BP Number: New BP13

Hosting Providers Deliverance of Secure Third Party Software:

Hosting Providers should take reasonable steps to provide secure and up to date third party website software and plug-ins for their customers. Software provided to customers should be actively supported for security fixes. Patching tools, processes or instructions should be provided to customers to help them keep their software current with security patches. Where feasible, select software that provides automatic security updates and provide customers with instructions on how to activate updates.

BP Reference/Comments:

TBD

BP Number: New BP13A

Hosting Providers Monitoring of Customer Environment:

Where feasible, Hosting Providers should monitor their environments for malicious or DDoS network traffic to identify sources of attacks.

BP Reference/Comments:

TBD

BP Number: New BP13B

Notify Hosting Customers of DDoS Traffic:

Hosting Providers, where feasible, should notify affected customers if malicious or DDoS network traffic is detected from their servers and, if appropriate, assist customers with remediation.

BP Reference/Comments:

TBD

BP Number: New BP14

Protect DNS against DDoS Attacks:

Service Providers should protect DNS services against DDoS attacks that would make DNS unavailable. Employ defense-in-depth strategies including, but not limited to:

- Deploy multiple servers with diverse network connectivity for each service such that any one server or site does not affect others.
- Configure network instrumentation to alert providers' operations teams to anomalous traffic volumes.
- Configure network to allow network and application level filtering of specific traffic (domains, query types, source IPs, query rates, etc.) during an attack; this must be configured in advance. This configuration must not interfere with legitimate DNS traffic.
- DNS servers must have out-of-band connectivity provisioned such that they can still be managed during an attack.
- Separate caching DNS servers from authoritative servers.
- Do not use Internet-facing DNS servers for network OAM&P systems.

BP Reference/Comments:

TBD