2014年9月

第5工作组
基于服务器的分布式拒绝服务攻击补救最终报告

目录

1 结果简介

1.1 执行摘要

关键基础设施部门受到了一系列分布式拒绝服务攻击的攻击，其中一些来自数据中心和托管服务提供商。来自数据中心和主机提供商的分布式拒绝服务攻击尤其成问题，因为攻击者可以使用高带宽和计算资源。这使得预防，发现和缓解更加重要，但也更加困难。该工作组研究了网络供应商和FCC可以采取的网络级最佳实践和其他措施，以减轻大型数据中心和托管站点的分布式拒绝服务攻击的影响并向理事会提出建议。这些建议包括促进利益相关方执行建议的技术/运营方法和程序。虽然本报告重点关注通信提供商，但需要指出的是，这需要跨互联网生态系统采取行动，包括主机提供商，设备提供商，关键基础设施所有者和运营商，依赖互联网的其他利益相关方甚至潜在的最终用户自己可以成功缓解分布式拒绝服务攻击。[1]
第5工作组还认识到，虽然基于服务器的分布式拒绝服务攻击在很大程度上不在本报告范围之内，但仍属于全国性问题。这是一个全球性问题。最终，互联网生态系统采取的行动包括国际考虑。

在这份最终报告中，第5工作组提出了一些建议，通信提供商可以采用这些建议来减轻数据中心和托管提供商（尤其是针对关键基础设施行业信息系统的分布式拒绝服务攻击）的分布式拒绝服务攻击的发生率和影响。这些建议主要以附录E中的基于服务器的分布式拒绝服务缓解最佳实践（BPs）的形式出现。此外，此处包含一些可行的建议，以进一步预防，检测和缓解基于服务器的分布式拒绝服务攻击。[2]

第5工作组还评估了互联网服务提供商实施BP的努力水平，与实施特定最佳实践的影响进行比较，以确定影响最大但实施水平相对较低的最佳实践的子集。该工作组还着重根据互联网服务提供商，互联网安全专家和金融社区子组的案例研究吸取经验教训，确定实施BP的障碍，并根据成员缓解分布式拒绝服务攻击的实际经验确定其他障碍。工作组还制定了一种分类法，以应用最佳实践。最后，小组讨论了潜在有效性措施，旨在衡量自愿网络级BP的成功结果，以减轻基于服务器的分布式拒绝服务攻击。

2 引言

这份最终报告记录了CSRIC IV工作组5所做的努力，并提供了通信提供商可以遵循的最佳实践，以减轻从通常基于数据中心和托管提供商的服务器发起的基于服务器的分布式拒绝服务攻击。最终报告还提供了有关FCC可以采取哪些措施来缓解此类威胁的建议。

[1] http://www.eweek.com/security/ddos-attacks-on-major-banks-causing-problems-for-customers/
[2] http://www.dhs.gov/critical-infrastructure-sectors

基于服务器的分布式拒绝服务攻击的发生和影响。

第五工作组由40多名成员组成的团队完成了CSRIC IV指控，其中包括来自ISP，金融机构，托管服务提供商，非营利组织，协会，学术界 ，联邦和州政府以及安全专家的代表。 CSRIC IV第5工作组的工作利用并补充了其他僵尸网络活动，包括：

- CSRIC II[3] 和CSRIC III[4]DDoS缓解建议
- 消息传递，恶意软件，移动反滥用工作组（M[3]AAWG）[5]
- 在线信任联盟（OTA）反僵尸网络工作组[6]
- 云安全联盟（CSA）[7]
- 工业僵尸网络集团（IBG）[8]

第5工作组研究了典型分布式拒绝服务攻击的基本结构，以及在当前网络环境中发现的不同类型的分布式拒绝服务攻击。图1显示了一个示例性的基于服务器的分布式拒绝服务攻击。最近的分布式拒绝服务攻击已利用网络托管公司和其他大型数据中心的漏洞向计算机系统和网站发起分布式拒绝服务攻击。这些攻击可以在国内或国际上以国内或国际目标发动。预防，检测和缓解这些攻击非常复杂，需要互联网服务提供商和网络运营商，数据中心和托管提供商，基础设施制造商（即供应链）以及关键基础设施所有者和运营商之间进行合作和信息共享。工作组以上述生态系统互动为基础，确定应对基于服务器的分布式拒绝服务攻击的缓解任务需要进行哪些案例研究，以及考虑采用哪些行业最佳实践。

3 http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-ii
4 http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii
5 http://www.maawg.org/m3aawg-san-francisco-meeting-addresses-latest-messaging-security-ranging-mobile-malware-ddos-attacks
6 https://otalliance.org/resources/botnets
7 https://cloudsecurityalliance.org/
8 http://www.ustelecom.org/blog/industry-botnet-group-takes-multi-party-approach-fight-cybercrime

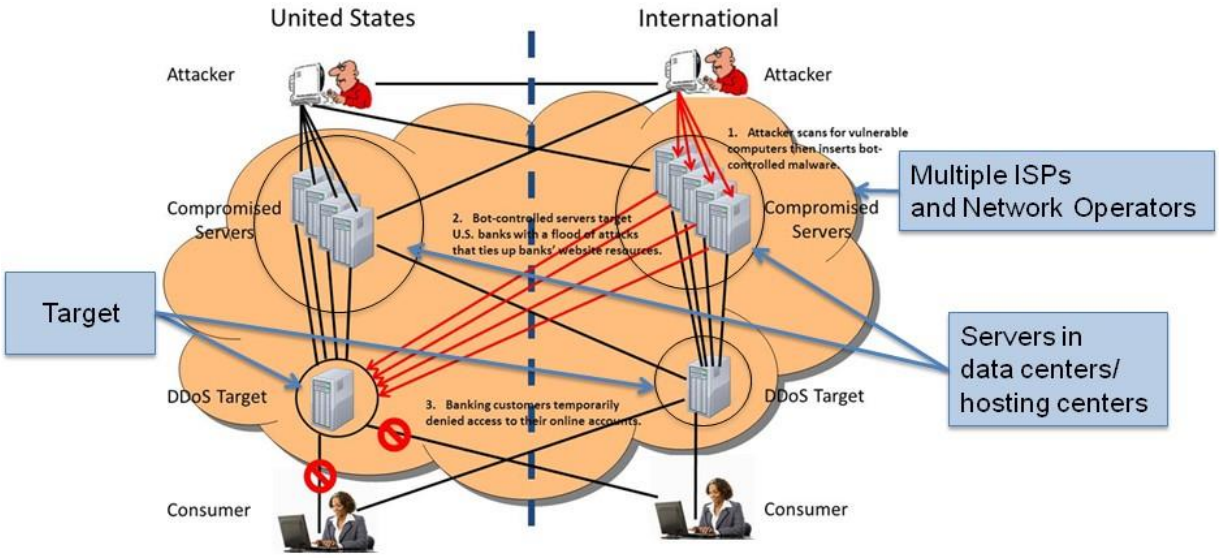


Figure 1 - Example of Server Based DDoS Attack

1

第5工作组还进行了差距分析，确定哪些最佳实践尚欠缺，但在哪些方面是必需的，以便与ISP事件响应生命周期的各个阶段保持一致，以保护和响应基于服务器的分布式拒绝服务攻击。在发现差距的地方，工作组就新的最佳实践提出了建议。

第5工作组将事件响应生命周期用作映射分布式拒绝服务最佳实践和建议的一种方法。这种映射以及每个领域的优先建议，将帮助互联网服务提供商确定每个领域最重要和有效的最佳实践和建议。在本最终报告中，工作组已将Arbor Network的“事件生命周期”调整为“分布式拒绝服务攻击准备和响应的六个阶段”，请参见下面的图2。

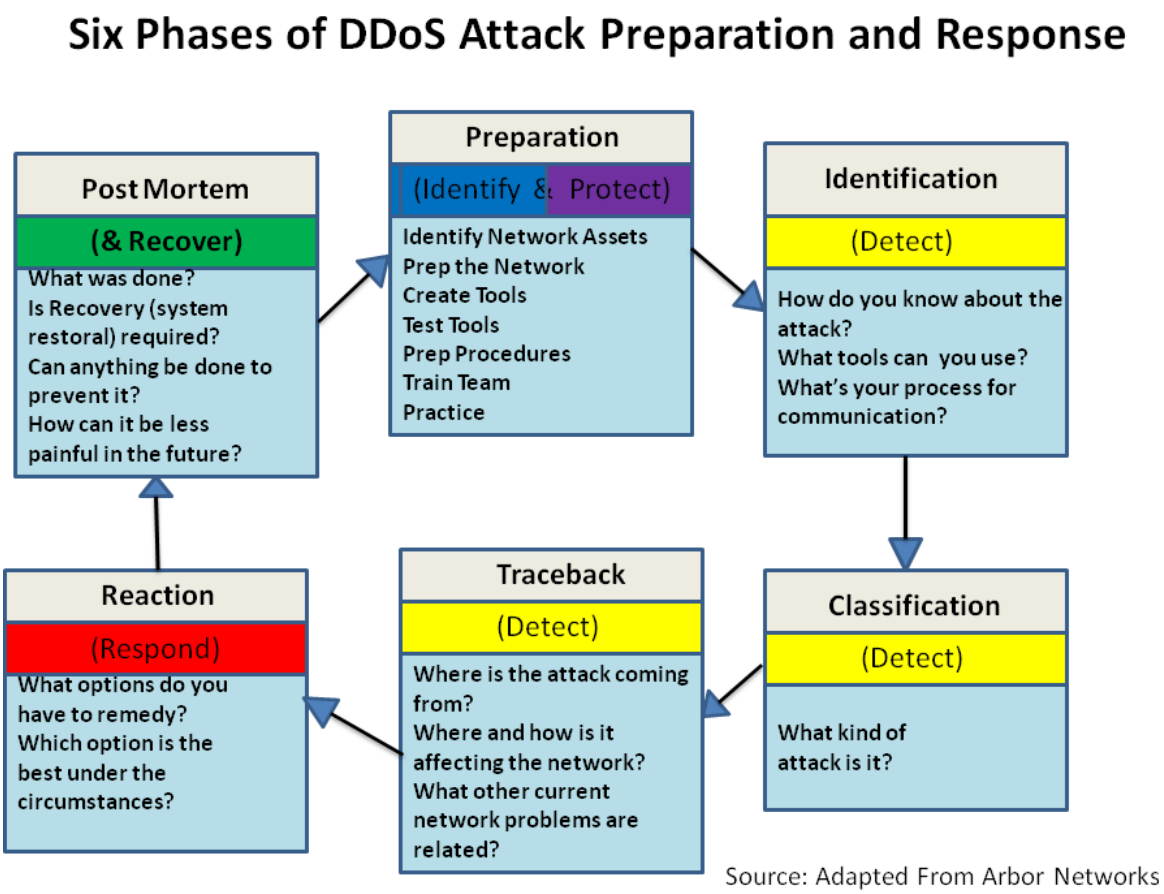


图2.分布式拒绝服务攻击准备和响应的六个阶段。

结合六个阶段模型，创建了活动分类法（附录A），以便为如何在每个阶段使用最佳实践提供指导。六个阶段模型是与NIST网络安全框架一致的攻击准备和响应方法。六个阶段操作模型与NIST网络安全框架相关，如下所示：准备阶段实现NIST识别功能以识别要保护的网络资产，并通过准备网络并创建分布式拒绝服务检测和缓解工具提供NIST保护功能。识别，分类和追溯阶段与NIST检测功能有关。反应阶段与NIST响应功能相关，后态阶段与NIST恢复功能相关。这种关系如下图3所示。[9]

[9] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

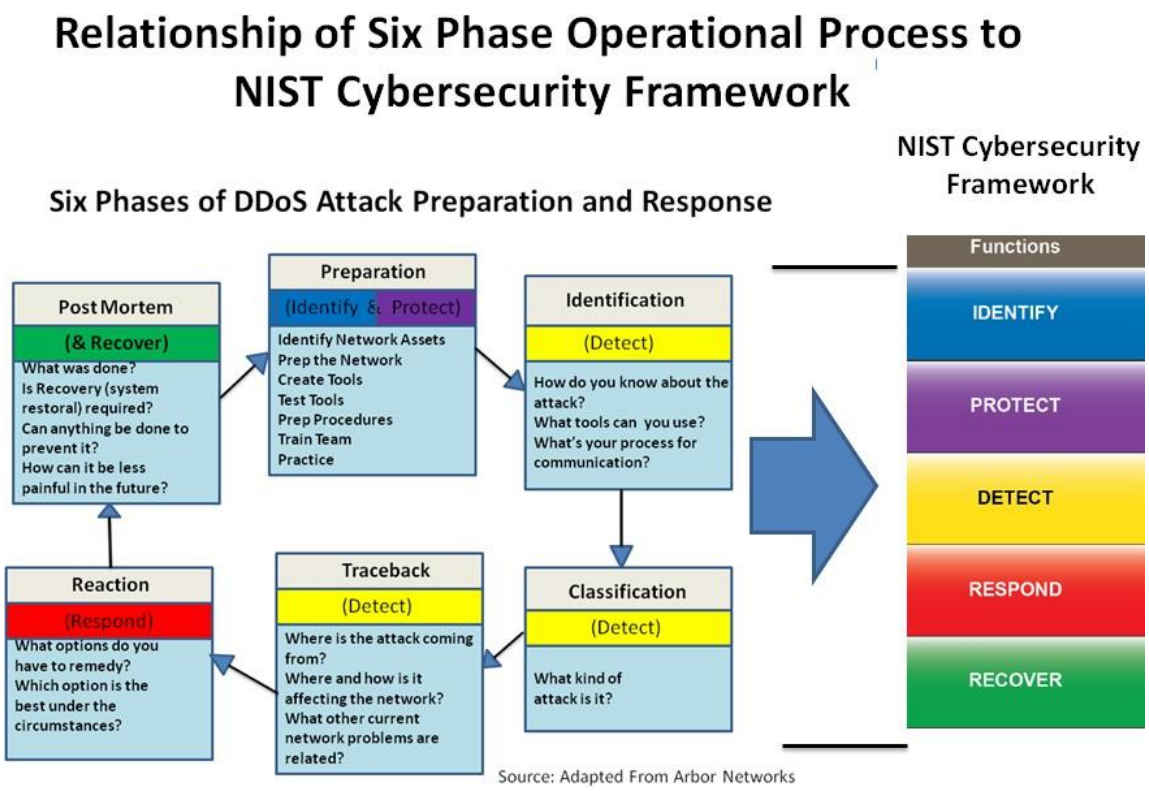


图3.六阶段运营流程与NIST网络安全框架的关系。

出于分析目的，工作组使用了以下定义的分布式拒绝服务攻击："拒绝服务（DoS）或分布式拒绝服务（DDoS）攻击是为了阻止合法用户访问信息或服务（美国CERT）。"分布式拒绝服务攻击由两个或多个同时攻击同一目标的系统或攻击者组成。以下是分布式拒绝服务攻击的类型：[10]

- 容量攻击
  - 直接数据包泛洪
    - 遭到破坏的远程控制计算机（机器人）将攻击流量直接发送到被攻击者，试图用不良流量填补电路。
    - 成百上万的机器人可以参与。
    - 标准的ISP工具可以很好地处理大多数此类攻击。
    - 数据包可以是伪造的，也可以不是伪造的。
  - 反射放大攻击
    - 僵尸机器人欺骗其源IP地址作为受害者的IP地址。
    - 将流量发送到服务，响应将比问题大得多。

[10] http://www.us-cert.gov/ncas/tips/ST04-015

- 域名系统（DNS）服务器是此类攻击的强大放大器。
- 放大倍数可达200倍以上。
- 数据包必须经过欺骗处理。

- 应用程序层攻击
  - 僵尸机器人恶意软件经过精心设计，可以将流量似乎来自合法客户和消费者大量计算机资源，发送到网络服务器或其他应用程序服务器。
  - 降低流量。
  - 攻击者需要更多的工作才能实现目标。
  - 加密流量更难缓解。
  - 全面缓解需要查看未加密的数据包。某些缓解措施仅适用于加密数据包
  - 通常无法欺骗数据包。
  - 域名服务（DNS）攻击
    - 域名系统是互联网上的两项关键服务之一，如果没有互联网服务，几乎所有互联网应用程序都会失败（邮件，网络等）。域名系统是互联网的白页。
    - 攻击者不是直接攻击受害者，而是攻击受害者的ISP DNS服务，减少受害者的流量。
    - 攻击不仅会影响受害者的流量，而且可能会影响许多其他ISP客户，即使这些客户可能不是攻击目标。

- 状态耗尽攻击
  - 保持连接状态的设备（如服务器，防火墙和状态检测功能有限的入侵检测/防御系统）。
- 控制平面攻击
  - 路由协议，如边界网关协议（BGP）和开放式最短路径优先（OSPF）。

工作组使用以上攻击类型确定了基于服务器的分布式拒绝服务攻击缓解最佳实践，并讨论了针对这些攻击的通用缓解工具和技术，形成了工作组建议的框架。

2.1 CSRIC IV结构

通信安全，可靠性和互操作性指标（CSRIC）IV									
CSRIC指导委员会									
主席或 联合主席： 工作中 第一组	主席或 联合主席： 工作中 第2组	主席或 联合主席： 工作中 第3组	主席或联合主席 讲座： 工作中 第4组	主席或 联合主席： 工作中 第5组	主席或联合主席 讲座： 工作中 第6组	主席或 联合 主席： 工作中 第7组	主席或 联合主席： 工作中 第8组	主席或联合主席 讲座： 工作中 第9组	主席或 联合 主席： 工作中 第10组
工作中 第一组： 下一个 世代 911	工作中 第2组： 无线网络 紧急情况 警报	工作中 第3组： EAS	工作中 第4组： 网络安全 最佳实践	工作中 第5组： 服务器 基于 分布式 拒绝服务 攻击	工作中 第6组： 长期的 核心互联网 协议 改进措施	工作中 第7组： 旧版 最好的 实践 更新	工作中 第8组： 潜水艇 电缆 着陆 网站	工作中 第9组： 基础设施 分享 在 紧急情况	工作中 组别 10：CPE 供电

表1 – CSRIC IV工作组结构。

2.2 第5工作组团队成员

第5工作组由以下成员组成。

名称	公司介绍
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	FSSCC
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
Errol Weiss	FSSCC
Pam Witmer	PA Public Utility Commission

表2-第5工作组成员列表。

3 目的，范围和方法

3.1 目的

该工作组负责就网络级最佳实践和其他措施减轻大型数据中心和托管站点的分布式拒绝服务攻击的影响，向理事会提出建议。工作组的目标是组织一个具有广泛经验和专业知识的工作组，包括政府和行业参与者。第5工作组的目标是：[11]

WG5目标

说明：

关键基础设施部门，包括金融部门，受到数据中心和托管服务提供商发来的分布式拒绝服务攻击的冲击。该工作组将审查网络级最佳实践和其他措施，以减轻大型数据中心和托管站点的分布式拒绝服务攻击的影响并向理事会提出建议。这些建议应包括技术和运营方法及程序，以促进利益相关方实施建议的解决方案。

可交付成果：

通信提供商可以采取建议措施，减轻数据中心和托管提供商的分布式拒绝服务攻击的发生率和影响，尤其是针对关键部门信息系统的攻击。

2

3.2 范围

近年来，分布式拒绝服务攻击的数量，规模和范围迅速增加，这给互联网服务提供商带来了挑战，因为

[11] http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC_IV_Working_Group_Descriptions_5_7_14.pdf

他们的网络。最近的攻击依赖于大数据托管中心内被感染的租户。为了解决基于服务器的分布式拒绝服务攻击问题，第5工作组采用了整体方法（例如，整个生态系统由多个利益相关方代表），重点是网络运营商可以采取的预防和缓解分布式拒绝服务攻击的措施。需要采用整体方法，因为分布式拒绝服务攻击的原因和影响需要由整个网络和托管生态系统解决才能生效。解决这一攻击媒介已成为所有生态系统利益相关方的优先事项。[12]

第5工作组的方法应尽可能做到包容各方，不要重复或重复其他小组为解决基于服务器的分布式拒绝服务攻击问题的其他方面而做出的努力。此外，第5工作组的方法应侧重于采取措施，特别是针对基于服务器的分布式拒绝服务攻击，建议采取行动，即，许多被认为是有价值的最佳实践，总体上是好的最佳实践，但不特定于服务器-
基于分布式拒绝服务攻击，因此不属于第5工作组的任务范围。其中一项建议是防范域名系统（DNS）拒绝服务攻击。重复和最近发生的域名系统攻击特别严重，因此，第5工作组的工作中包括了缓解风险的最佳实践。[13]

3.3 方法论

第5工作组从确定子组开始，适当关注基于服务器的分布式拒绝服务攻击案例研究和行业最佳实践分析。从这一重点得出以下四个子小组：ISP，金融社区，互联网安全专家和最佳实践子小组。

最佳实践分组确定了适用于基于分布式拒绝服务服务器攻击的BP，而互联网服务提供商，金融社区和互联网安全专家分组针对基于服务器的分布式拒绝服务攻击制定了具有代表性的案例研究。然后，由第5工作组在大型网络中与每个子组区域相关联的最佳实践，以及其他措施，以缓解大型数据中心和托管站点的分布式拒绝服务攻击的影响。

第5工作组与工作组成员每两周举行一次电话会议以完成任务。此外，各小组每两周举行一次电话会议，征求意见并审查案例研究可交付成果。第5工作组于2014年1月（弗吉尼亚州阿灵顿）和2014年4月（科罗拉多州朗蒙特）举行了为期两天的面对面会议，于2014年7月（弗吉尼亚州阿灵顿）举行了最后一次面对面会议。，以促进对可交付成果的讨论。

第5工作组审核了大约600个网络安全BP，以确定它们是否属于工作组的任务范围（即，缓解基于服务器的分布式拒绝服务攻击的BP）。工作组将适用清单减少到大约30个突出BP。工作组结合NIST网络安全框架，使用分布式拒绝服务攻击准备和响应的六个阶段进行了差距分析。根据差距分析，工作组还编写了一些新的业务流程，供通信行业自愿采用。

12？http://www.darkreading.com/attacks-and-breaches/bank-attackers-used-php-websites-as-launch-pads/d/d-id/1107833
13http://www.pcworld.com/article/2040766/possibly-related-ddos-attacks-cause-dns-hosting-outages.html

工作组还根据亚组案例研究总结的经验以及成员经验，确定了实施BP的障碍，并考虑了基于结果的有效性指标，这些指标表明了是否自愿开展基于服务器的分布式拒绝服务攻击具有良好的效果。工作组还采用了“六阶段分类法”（附录A）作为确定实施候选最佳实践的指南。

最后，工作组就FCC采取的行动提出建议，通过更广泛地采用建议的基于服务器的分布式拒绝服务最佳实践，帮助缓解分布式拒绝服务攻击的影响。

3.3 指标

在确定遵循本报告中推荐的最佳实践的有效性方面，成功衡量基于服务器的分布式拒绝服务攻击至关重要。第5工作组成员认识到，采用一致，统一的方法来衡量遵循推荐BP的有效性，将为确定是否需要在整个生态系统中采取其他自愿行动，从整体上应对基于服务器的分布式拒绝服务攻击奠定基础。

第五工作组还认识到可能难以实现有效措施。每个网络运营商都有不同的方法来处理分布式拒绝服务攻击。建立共同的成功衡量标准要求参与者建立统一的方法来收集，解释，分析和报告分布式拒绝服务攻击指标。为了衡量遵循建议的基于服务器的分布式拒绝服务攻击BP的有效性，必须谨慎选择指标，以有意义，可测量和可重复的方式衡量预期结果。认真分析整个生态系统的总体指标，并推断实施建议的BP的有效性，需要所有有助于收集，分析，报告和解释指标的生态系统利益相关方参与和合作。

为了让更广泛的生态系统参与者参与统一的方法来衡量实施推荐的BP的有效性，第5工作组与CSRIC IV的第4工作组（网络安全最佳实践）合作，以利用其100多名成员，全面解决指标，衡量实施建议的BP的有效性，不仅适用于基于服务器的分布式拒绝服务攻击，也适用于其他建议的网络安全BP。第5工作组成员将与第4工作组成员联系，完成这项整体指标工作，纳入2015年3月交付的第4工作组。

作为第4工作组衡量指标工作的一部分，第5工作组将建议潜在的基于服务器的分布式拒绝服务攻击指标，可以将其视为测试案例，供整个生态系统参与者考虑。这些措施由第5工作组成员确定，对第4工作组而言，对于衡量在整个生态系统中遵循建议的基于服务器的分布式拒绝服务攻击BP的有效性至关重要，并且在概念上是可行的试验措施以便由第4工作组建立严格的审查流程。

3.4 参与障碍

以下各节介绍了第5工作组在采用本文档中建议的最佳实践方面在网络运营商参与障碍方面所做的努力。这些部分主要根据CSRIC III的ISP代码参与指南进行改编，因为遵循CSRIC III工作组7推荐的《美国ISP自愿反机器人行为守则》确定的障碍适用于网络运营商在遵循第5工作组推荐的服务器时可能遇到的障碍基于分布式拒绝服务攻击的BP。除了网络运营商，在建议的BP适用的范围内，托管服务提供商也可能遇到类似的障碍。CSRIC III完成的先前工作为第5工作组克服障碍提供了适当的定义和框架。[14]

这份最终报告中提供的许多建议最佳实践涉及不同级别的承诺和复杂性。众所周知，私营部门参与者在内部争夺投资资本和人力资源，对此类投资进行优先排序的决策越来越依赖于向决策者提供坚实的业务案例。

《障碍指南》旨在通过提供与具体建议相关的结构化资源集，包括实施方面的最佳可用指南，鼓励更广泛的参与。

3.4.1 参与障碍：考虑因素

在必要活动影响多个组织的现有方法和程序以及资源的范围内，采用最佳实践可能会造成障碍。网络运营商不仅需要了解可能需要进行哪些更改，还需要从流程，资源和预算角度了解哪些组织受到影响。必须考虑可伸缩性和部门间集成级别，以及实施建议所需的任何持续支持。在解决障碍时，我们努力将每个已识别的障碍归为以下类别之一：

3.4.1.1 技术壁垒

技术壁垒是指在当前技术解决方案可能不足以应对威胁或这些解决方案可能具有其他不可接受的副作用的情况下的障碍。技术解决方案作为障碍的重要性取决于实施特定建议所需的技术程度。某些解决方案可能需要最少的技术资源（资产和人员），而其他解决方案可能要求更高，包括系统集成级别。实施建议的方式还可能取决于网络运营商当前的现状，包括内部能力，资源和优先级或对第三方资源的访问。技术壁垒可能直接转化为财务障碍。可能存在技术解决方案，但在网络运营商中实施该解决方案的成本可能过高。

[14] http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf

3.4.1.2 客户/市场壁垒

客户或市场壁垒是实施解决方案时产生的壁垒，客户可能认为其无效（例如，客户选择不参加）或不受欢迎（例如，隐私，限制性条款和条件）。网络运营商的活动也可能会在市场上产生后果，包括提高产品成本，网络运营商愿意投入的资本投资，客户购买解决方案的意愿以及与竞争产品相关的其他考虑因素。实施作为托管安全服务提供的一些最佳实践，将是网络运营商的业务决策。他们将需要决定是否希望提供这些服务，如果愿意，内部或通过第三方实施这些服务。最后，他们需要确定最能与其竞争所在市场相匹配的托管安全服务产品的范围，功能，容量和价格。

3.4.1.3 运营壁垒

运营壁垒是可能会对组织的主要使命和资源产生不可接受的影响的壁垒。承担运营责任的组织通常会通过定义明确的绩效指标负责。
（例如，客户服务代表的平均交易时间）。任何新的运营实践都必须充分注意以下几点：

- 开发和更新操作方法和程序；
- 重新分配现有或额外资源；
- 解决方案的可扩展性；
- 运营绩效目标，关键的成功因素和衡量结果的能力。

3.4.1.4 财务障碍

财务壁垒是由于无法量化与实施特定建议相关的成本或收益。在当前的经济环境下，缺乏针对公司的业务案例可能是采用该业务的重大障碍。私营部门公司负有信托责任，基于审慎的资本配置做出决策。在部署与安全相关技术的投资时，大多数公司依靠可量化数据对系统，流程和人力资源上的新投资进行优先级分配。

3.4.1.5 法律/政策壁垒

禁止网络运营商之间协作和信息共享的法律
（美国或国外）可以掩饰恶意行为者。恶意行为者有能力[15]

15参见编号。

将僵尸网络伪装为合法流量，会使安全专业人员处于无法维持的地位，有可能侵犯最终用户对隐私的期望，或者允许进行危险且昂贵的犯罪活动。此外，即使被认为是恶意流量，网络运营商也不一定能够阻止流量。例如，流量可以与商业活动交织在一起，这样，缓解措施的成本就要大于僵尸网络造成的危害。网络运营商在为客户提供保护，保护客户隐私和尊重其他网络运营商期望的自治权之间一直面临着持续的平衡。16

3.4.1.6 障碍-基于服务器的分布式拒绝服务攻击

来自数据中心和主机提供商的分布式拒绝服务攻击尤其成问题，因为攻击者可以使用高带宽和计算资源。这使得预防，发现和缓解更加重要，但也更加困难。基于服务器的分布式拒绝服务攻击需要生态系统的参与，甚至比其他类型的攻击更大。
基于服务器的分布式拒绝服务攻击的这些方面给应对攻击带来了特殊的障碍。本报告提供了一些新的最佳实践，针对这些方面以及现有的和最新的最佳实践。通常，以下是针对基于服务器的分布式拒绝服务攻击的特殊考虑因素的陈述：

3.4.1.6.1 技术注意事项：

本文档中确定的一些最佳实践很难或无法在某些网络中实现（不影响某些网络），具体取决于网络体系结构。本文档中概述的一些最佳实践部分取决于某些网络设备平台上可用的技术，但不取决于其他平台。

3.4.1.6.2 客户/市场注意事项：

一些最佳实践虽然非常有效，却是客户必须购买和配置的附加服务。攻击缓解控制可能会干扰合法流量，对于客户而言，这可能是不可接受的。

3.4.1.6.3 运营注意事项：

尽管许多最佳实践本身并不难实现，但成千上万个客户的规模实施会带来配置管理和后台系统方面的极大复杂性。某些缓解技术可能会对同一数据中心内的其他客户造成附带损害，数据中心运营商可能认为这是不可接受的。许多运营更改建议均要求网络运营商与其客户进行协调，以避免中断。如果客户没有直接从实施中受益，那么这将是一笔巨大的时间投资，也可能导致客户留存问题。

3.4.1.6.4 法律/法规/政策注意事项：

16参见《我们能否击败僵尸网络模仿合法网络行为模仿攻击》，IEEE（2012年）。

在一些制定严格本地隐私法律的国家/地区，提供商之间的数据共享可能会更加困难。关于攻击期间共享的不准确数据，也可能存在责任问题。

3.4.1.6.5 财务考虑：

本文档中的许多最佳实践取决于特定的功能和功能集，这些功能在路由器中并不普遍存在。实施可能需要网络运营商，主机提供商或客户购买新设备。
某些已识别最佳实践的实施可能会影响网络设备或服务器的性能。反过来，这可能需要功能更强大或更多的设备，使所有客户的服务成本更高。

4 背景资料

先前的CSRIC已经推荐了最佳实践，可用于缓解拒绝服务和分布式拒绝服务攻击。
CSRIC II批准了第8工作组在其最终报告《 ISP网络保护实践》中的建议：*17*

- 在预防，检测，通知，缓解和隐私考虑方面的推荐最佳实践（BPs）
- 重点关注为住宅宽带网络上的消费者提供服务的互联网服务提供商的BP，但注意到报告中确定的许多最佳实践也将是适用于非消费者，非住宅网络环境的宝贵实践
- 进一步建议，FCC稍后再考虑在非住宅环境下开展额外的最佳实践工作是否有价值。

CSRIC II还批准了2A工作组的最终报告中的建议
网络安全最佳实践：18

- 更新了网络安全最佳实践，反映了通信行业当前的技术环境，并通过以下方式提供了相关参考资料：
  - 分析现有的NRIC，NIST，SANS，IEEE等与网络安全相关的最佳实践
  - 建议对现有的最佳实践进行修改和删除
  - 识别通信行业现有技术和相对新技术的新网络安全最佳实践。

CSRIC III批准了第7工作组在其最终报告《美国互联网服务提供商的反机器人行为守则》（互联网服务提供商的ABC）中的建议：*19*

- 专注于住宅宽带设备带来的僵尸网络威胁
- 建议的ISP在教育，检测，通知，补救和协作领域的自愿措施

17
http://www.fcc.gov/pshs/docs/csric/CSRIC_WG8_FINAL_REPORT_ISP_NETWORK_PROTECTION_20101213.pdf
18http://www.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf
19http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-ReportFinal.pdf

- 进一步建议FCC与其他联邦政府机构和行业合作，促进有关僵尸网络缓解活动的案例研究的创建

CSRIC III通过了第四工作组在其最终报告“ DNS最佳实践”中的建议：*20*

- 在实施DNSSEC之前，专注于最佳实践，以保护互联网域名系统和路由系统。

CSRIC III还批准了第5工作组的最终报告中的建议
ISP的DNSSEC实施实践：21

- 检查由互联网服务提供商（ISP）部署和管理域名系统安全扩展（DNSSEC）的最佳实践。
- 建议适当的指标和度量，以便评估互联网服务提供商（ISP）部署DNSSEC的有效性。

最近的分布式拒绝服务攻击已利用网络托管公司和其他大型数据中心的漏洞向计算机系统和网站发起分布式拒绝服务攻击。 CSRIC
IV认识到，为了影响这些最新的分布式拒绝服务威胁，这方面的工作既及时又重要。根据先前的CSRIC专注于住宅网络的进展情况，CSRIC
IV第5工作组获得了章程，建议通信提供商采取措施减轻数据中心和托管提供商的分布式拒绝服务攻击的发生率和影响，特别是针对数据中心和托管提供商的分布式拒绝服务攻击关键基础设施部门的信息系统。22

5 分析，发现和结论

5.1 分析

案例研究着眼于许多基于服务器的分布式拒绝服务攻击。攻击可能涉及多个ISP，多个数据和托管中心。

- 基于服务器的分布式拒绝服务攻击剖析

如图3所示，攻击者可以控制数据中心和托管服务器，并利用可观的计算和网络资源向企业受害者发起分布式拒绝服务攻击。请注意，目标也可能是互联网服务提供商基础设施的一部分。此类攻击会淹没对目标的访问，拒绝合法用户的访问，并导致

20
http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf
21
http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG5_Report_March_%202013.pdf
22启动板/ d / d-id / 1107833？http://www.darkreading.com/attacks-and-breaches/bank-attackers-used-php-websites-as-

通过影响分布式拒绝服务流量路径上的其他各方，造成附带损害。缓解此类攻击需要所有相关各方采取行动：

- 多个ISP
- 托管服务提供商/数据中心/代理商
- 目标基础设施
- 发起攻击者的ISP基础设施

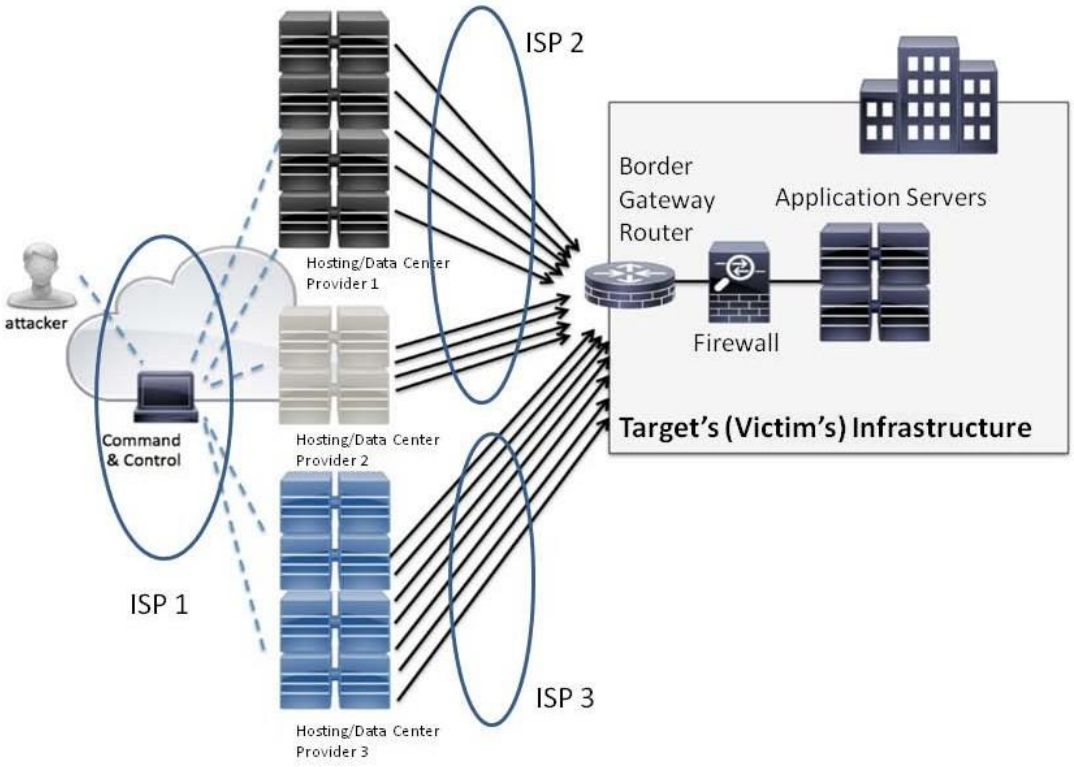


图3 –基于服务器的分布式拒绝服务攻击。

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

- 攻击分类法–
  创建了基于服务器的分布式拒绝服务攻击类型的分类法，以确定缓解攻击所需的防御范围。攻击分类法包含在附录C中。

- 个案研究
  - 第5工作组确定了三个小组，重点研究基于利益相关方服务器的分布式拒绝服务攻击案例研究，第四个小组进行行业最佳实践分析。子类别为：互联网服务提供商，金融

社区，互联网安全专家和最佳实践子组。
  - 最佳实践分组确定了适用于基于分布式拒绝服务服务器攻击的BP，而互联网服务提供商，金融和互联网安全专家分组针对基于服务器的分布式拒绝服务攻击制定了具有代表性的案例研究。案例研究包含在附录D中。

- 建议最佳实践
  - 最佳实践包含在附录E中

5.2 调查结果

案例研究的关键发现：

1. 分布式拒绝服务攻击规模越来越大，足以压垮单个互联网服务提供商的吸收能力。
2. 基于服务器的攻击利用数据中心计算和网络资源进行前所未有的大规模分布式拒绝服务攻击。
3. 由于分布式拒绝服务攻击数量的增加，附带损害（对非分布式拒绝服务攻击目标的其他人的影响）很常见–
   数据包丢失，延迟，无参与方的互联网流量高延迟，而这些流量恰好穿越了这些攻击所饱和的网络。
4. 分布式拒绝服务攻击不仅用于中断服务，而且在尝试其他攻击（例如欺诈性交易）时分散安全资源。
5. 自适应分布式拒绝服务攻击很普遍。攻击者会实时改变攻击流量，以避免识别身份，并挑战和混淆缓解策略。
6. 反射和放大攻击仍然很普遍，利用配置错误的域名系统（DNS），网络时间协议（NTP）和其他网络资源，能够欺骗（伪造）源（目标）IP地址。
7. 僵尸网络体系结构变得越来越复杂，跟踪和命令控制（C2）系统越来越多地使用代理服务器和对等网络来混淆执行命令的系统位置。此外，某些僵尸网络有能力在完成攻击后破坏受感染的系统。
8. 设备在全球范围内越来越分散，由于各国法律通常不同，有时甚至相互矛盾，因此很难协调关闭这些系统。
9. 分布式拒绝服务流量快速建立，因此需要自动缓解功能来保护基础设施。
10. 为了支持自动缓解功能，需要遵循标准化的分类法来表达缓解基于分布式拒绝服务服务器的攻击所需的信息。
11. 需要更广泛地部署反欺骗（anti-forging）技术，防止放大攻击。
12. 分布式拒绝服务缓解功能需要在整个网络中部署，因为很难预测攻击的来源。
13. 分布式拒绝服务缓解需要多个工具。互联网服务提供商需要目的黑洞过滤功能才能保护网络，因为他们意识到黑洞过滤可以完成网络攻击。

分布式拒绝服务攻击目标。攻击缓解程序需要多种类型的侵入性较小的功能，才能最大程度地降低分布式拒绝服务攻击的有效性。

14. 分布式拒绝服务攻击需要整个网络生态系统应对，而不仅仅是网络运营商。其中包括托管中心和数据中心提供商，分布式拒绝服务目标，软件供应商，开源组织以及设备制造商（整个供应链）。
15. 分布式拒绝服务缓解需要目标，主机提供商和网络运营商紧密合作。随着新型分布式拒绝服务缓解技术越来越有效，攻击者将继续调整其技术，找到攻击目标的新方法。
16. 不仅要由网络运营商，而且要由更广泛的互联网生态系统利益相关者解决为确定遵循基于服务器的自愿性分布式拒绝服务攻击最佳实践的有效性而采用的潜在成功措施，以便对有效性进行有意义的整体解释。

5.3 结论

在这份最终报告中，第5工作组记录了调查结果，提出了建议，提出了应对基于服务器的分布式拒绝服务攻击的最佳实践，解决了实施中的障碍，并提出了一条全面解决遵循推荐的BP措施的措施。我们在这份最终报告中总结道，不仅需要网络运营商采取行动，而且需要采取措施预防，检测和缓解攻击，这是受到基于服务器的分布式拒绝服务攻击影响的利益相关方的整个生态系统。

6 建议

1- FCC鼓励互联网服务提供商考虑按优先级顺序自愿实施建议的最佳实践和新建议（附录E），以通过提高对这些最佳实践的认识和收益来应对基于服务器的分布式拒绝服务攻击。
2- FCC鼓励主机托管提供商开发最佳实践，以促进安全计算实践，减少漏洞并减少利用漏洞的威胁，从而减少基于服务器的分布式拒绝服务攻击的发生率。
3- FCC鼓励对等方之间自愿建立的私营部门关系（若不存在），就分布式拒绝服务响应最佳实践和缓解支持进行合作。
4- FCC鼓励在现有DHS信息共享结构内开发一个自愿中央数据交换中心，为分布式拒绝服务缓解信息，可以作为ISP，托管提供商，目标，响应组织（CERTS和ISAC）和政府之间的资源，实时缓解分布式拒绝服务攻击。
5- FCC鼓励生态系统利益相关方在彼此之间或通过使用标准化分类法（如结构化威胁信息表达（STIX）或类似结构）的集中式票据交换所共享基于分布式拒绝服务服务器的攻击信息，以帮助自动缓解攻击。[23]
6- FCC鼓励共享分布式拒绝服务缓解最佳实践，威胁，漏洞，

[23] https://stix.mitre.org/

以及Comm-ISAC中网络运营商之间的事件响应操作。

7 致谢

这份最后报告反映了所有工作组成员的宝贵贡献。第5工作组联合主席，CenturyLink的DHS和美国国土安全部局长Peter Fonash表示感谢，第5工作组的所有成员辛勤工作，投入大量时间和精力，最终完成了本最终报告。共同主席谨向感谢Century Link的保罗·戴蒙德（Paul Diamond）和Bell Labs的罗伯特·桑伯里（Alcatel Lucent）两位编辑的不懈努力，Alcatel Lucent 在编写中期和最终报告方面做出了杰出贡献。共同主席还想表彰以下是重要小组工作的领导人：

- 互联网服务提供商– Verizon的Jared Allison和AT&T的Chris Boyer
- 金融–美国银行的John Denning 和金融服务部门协调理事会（FSSCC）的埃Errol Weiss
- 互联网– Arbor网络公司的Roland Dobbins
- 最佳实践–Alcatel–Lucent 和 Bell Labs的Robert Thornberry

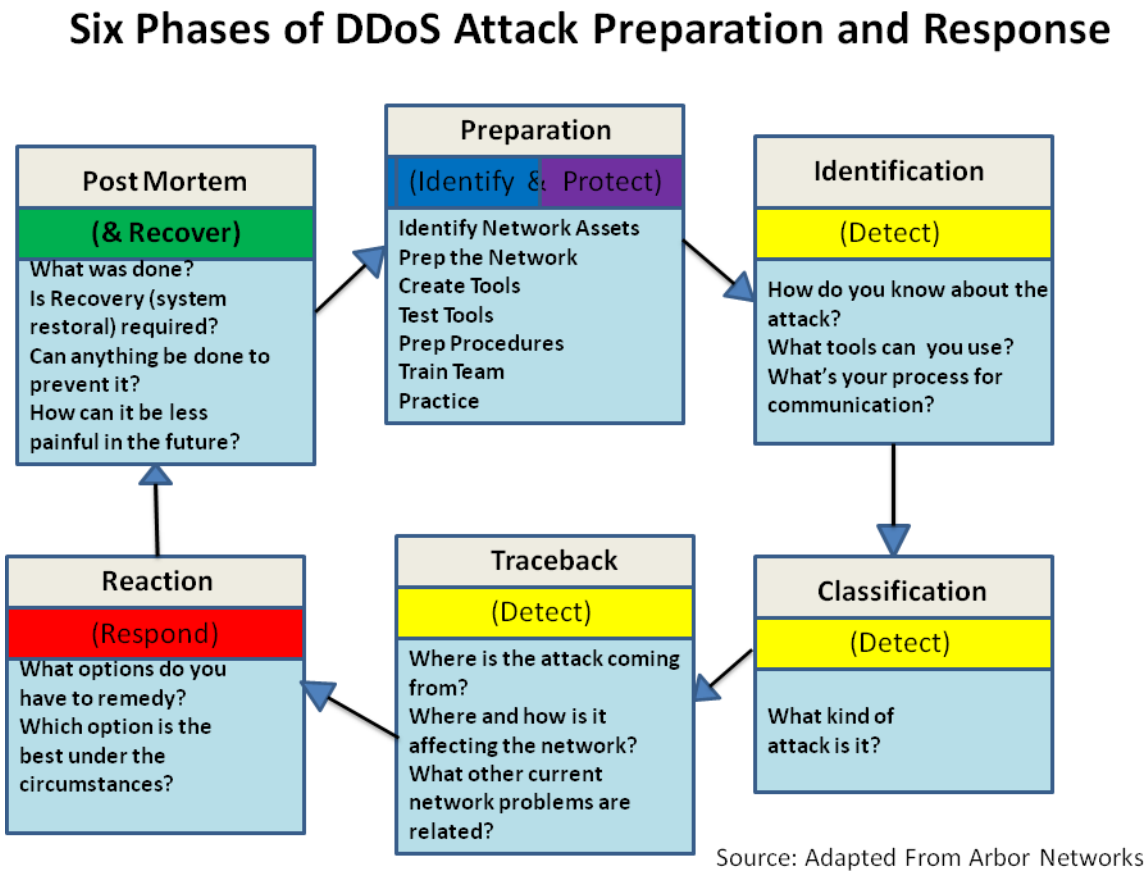
共同主席要感谢联邦通信委员会的VernonMosley在促进编写报告方面做出的巨大努力。共同主席还感谢主持人CenturyLink和Intrado面对面的会议。共同主席也要感谢CAUCE的Jo hn Levine建立和维护WG5 Wiki和Listserve。

第5工作组成员要感谢联席主席Michael Glenn和Peter Fonash的出色领导，他们保持工作组专注并创建高性能团队环境，为基于服务器的分布式拒绝服务做出贡献攻击缓解建议。

8 附录

附录A：分布式拒绝服务攻击准备和响应分类的六个阶段
附录B：基于服务器的分布式拒绝服务术语表
附录C：分布式拒绝服务攻击分类
附录D：分布式拒绝服务攻击缓解案例研究
附录E：基于服务器的分布式拒绝服务攻击最佳实践

附录A：分布式拒绝服务攻击准备和响应分类的六个阶段



Source: Adapted From Arbor Networks

准备工作
沟通交流
ISP和Pure Play分布式拒绝服务
缓解公司（PP）
ISP / PP到ISP / PP
ISP / PP到托管
ISP / PP对受害者
ISP / PP到中央协调
中心
托管
托管到ISP
托管到托管
托管到受害者
主持中央协调
中心
目标
ISP的受害者
被托管的受害者
从被害人到被害人
目标到中央协调中心

监控和可见性
互联网服务提供商
网络流量
流量级别
服务器基础设施资源级别
路由劫持
固件，路由器，服务器日志
托管
网络流量
流量级别
服务器基础设施资源级别
ISP攻击信令
固件，路由器，服务器日志
目标
服务器基础设施资源级别
ISP攻击信令
固件，路由器，服务器日志

预防措施
互联网服务提供商
反欺骗技术
减少反射面
速率限制/流量阻止
托管
反欺骗技术
减少反射面
速率限制/流量阻止
服务器资源最小化计划和过程

目标

服务器资源最小化计划和过程

部署和配置缓解工具

ISP和Pure Play分布式拒绝服务缓解公司过滤

CDN过滤（网络流量攻击）
BGP Flowspec
黑洞过滤（信号源和
目的地）
网络数据清理
托管过滤
现场数据清理
目标过滤
现场数据清理

容量和资源
互联网服务提供商
域名服务器
域名系统网络容量
BGP链接，路由器和状态
保护
托管
域名服务器
域名系统网络容量
BGP链接，路由器和状态
保护
数据中心上行带宽
防火墙，IDS / IPS，交换机容量
目标
服务器和网络上行链路
防火墙，IDS / IPS，交换机容量
服务器资源容量

最小化攻击服务

互联网服务提供商
关闭打开的域名解析器
限速域名系统查询
速率限制开放协议（NTP，回显，等）
关闭不必要的协议
网络基础设施
托管
关闭打开的域名解析器
限速域名系统查询
速率限制开放协议（NTP，回显，等）
关闭不必要的协议
网络基础设施
关闭不必要的协议
服务器和虚拟基础设施
目标

关闭不必要的协议
服务器和虚拟基础设施

对等和上游ISP合作缓解协议

正式和非正式
缓解协议
识别24/7
对等或上游互联网服务提供商（ISP）的运营联系人，提供攻击缓解帮助

身份证明
监控和可见性
互联网服务提供商
Netflow（带有路由器和接口信息）
流量级别
服务器基础设施
路由劫持
固件，路由器，服务器日志
完整的数据包捕获和分析
托管
Netflow（带有路由器和接口信息）
流量级别
系统负载
ISP攻击信令
固件，路由器，服务器日志
完整的数据包捕获和分析
目标
系统负载
ISP攻击信令
固件，路由器，服务器日志
完整的数据包捕获和分析
与目标确认
（客户）流量是真正的攻击流量。

分类

攻击类型
容量攻击？
直接数据包泛洪
反射/放大
应用程序层攻击？
状态或资源
力竭攻击？

控制平面攻击？

Ipv6特定攻击？

追溯
标识源IP

入口路由器接口的标识

分布式拒绝服务数据包路径的标识

中间流量负载

识别反射面（路由器，服务器等）

入口路由器的标识
欺骗性反射数据包的接口

反应

确定最佳工具或一组工具来缓解攻击

分析目标为微调缓解过滤器的剩余流量以及攻击流量和方法的变化

监控过滤方法，最大限度地减少误报流量

是否需要对等或上游提供商的帮助以减轻攻击？

后形态

如何快速识别和分类攻击？

这些工具在缓解攻击方面是否有效？

是否有其他预防措施可以预防将来的攻击？

是否可以采取其他缓解措施来更有效地缓解未来的攻击？

沟通是否及时有效？

是否需要相互ISP互助协议？有效吗？

附录B：CSRIC IV WG5基于服务器的分布式拒绝服务术语表

（本词汇表结合了CSRIC III WG7最终报告中的词汇表作为基准。）

I. 条款：

1. 黑洞过滤/黑洞路由

一种用于根据源或目标IP地址删除网络流量的技术。黑洞过滤/路由通常用于缓解网络运营商的拒绝服务或分布式拒绝服务攻击。这项技术可以部署在边缘，边界或核心路由器上，以有效地将攻击流量丢弃到网络入口点附近，以最小化攻击对网络或其他客户流量的影响。

2. 僵尸机器人

恶意（或潜在恶意）“机器人”（源自“机器人”一词，以下简称为“机器人”）指的是安装在系统上以使系统能够自动（或半-自动）通常在远程管理员（通常称为“僵尸机器人”或“僵尸机器人”）的命令和控制下执行一项或一组任务。

被“破坏”的计算机系统和其他最终用户设备通常也称为“僵尸”。

恶意机器人通常在未经用户同意的情况下秘密安装，或者在用户未完全了解机器人安装后可能会做什么的情况下进行秘密安装。

僵尸机器人通常用于发送垃圾电子邮件，侦听或攻击其他系统，窃听网络流量或托管非法内容，例如盗版软件，儿童剥削材料等。

许多司法管辖区都认为，最终用户主机的非自愿感染是非法入侵计算机的一个例子。

3. 僵尸网络

僵尸网络是指感染了僵尸恶意软件的互联网连接终端用户计算设备网络，由第三方出于恶意目的进行远程控制。
僵尸网络受指定的“ botherder”或“ botmaster”控制。一个僵尸网络可能只有少数几个僵尸主机，甚至数百万个。

4. 通讯提供商

通信提供商包括互联网服务提供商，服务提供商，网络运营商，托管中心运营商，数据中心运营商以及支持这些提供商的制造商生态系统。

5. 客户（或“直接客户”）

与ISP签订服务合同的一方。区分“客户”与“授权用户”：例如，一家咖啡店可以从ISP购买互联网服务。咖啡店将是ISP的客户。咖啡店可以选择免费使用其连接（如果

由ISP的“可接受使用政策”（AUP）允许向从中购买咖啡的用户允许-咖啡购买者将被视为咖啡店购买连接的授权用户，但不是ISP的直接客户。

6. 数据中心

一种设施，专用于在提供高可用性电源和网络功能的环境中容纳大量计算和网络资源。

7. 数据清理

将拒绝服务或分布式拒绝服务攻击流量路由到系统或服务，试图区分“正常”网络流量和攻击流量，并在传递正常流量时丢弃攻击流量。数据清理器可以部署在网络运营商的网络或客户驻地。对于大于客户驻地带宽的攻击流量，需要使用基于网络的数据清理器有效缓解攻击。

8. 拒绝服务（DoS）或分布式拒绝服务（DDoS）攻击

拒绝服务（DoS）或分布式拒绝服务（DDoS）攻击是为了阻止合法用户访问信息或服务（US-CERT）。分布式拒绝服务攻击由两个或多个同时攻击同一目标的系统或攻击者组成。[24]

9. 检测

检测是服务提供商或最终用户意识到特定系统或设备已感染恶意软件的过程。服务提供商可能会以多种不同方式检测到系统感染病毒，包括接收到来自第三方的有关垃圾邮件，网络扫描或源自该系统的攻击的投诉。最终用户可以通过软件工具或其他手段检测系统感染。

10. 生态系统

该术语通常用于描述各种互联网参与者之间的相互关系，硬件制造商，软件开发人员，互联网服务提供商（ISPs）和各种使互联网运转并对终端用户有用的互联网内容，应用和服务的提供商。

互联网生态系统包括操作系统供应商，面向最终用户的组织，互联网内容，应用程序和服务提供商，ISP，搜索提供商，最终用户，IT部门，托管公司，博客提供商，安全提供商，研究人员，政府，金融服务公司和其他各方。

所谓的“地下经济”也经常被描述为“生态系统”，多个参与者扮演着不同的专门角色。例如，一些参与者可能专注于编写恶意软件，而其他参与者可能会“收获”网页和邮件列表中的电子邮件地址，而另一些参与者可能专注于将恶意软件分发给那些收获的电子邮件地址。
恶意软件生态系统通常还将包括目标潜在受害者的人群，以及致力于打击网络犯罪的执法机构。

[24] http://www.us-cert.gov/ncas/tips/ST04-015

11. 最终用户

最终用户：在计算和网络环境中，最终用户是指最终授权使用产品或服务的人。

最终用户通常可能与购买产品或服务的人不同。例如，一家咖啡店所有者可以购买连接服务，供其客户使用；在这种情况下，即使他们没有直接与ISP签定使用连接的连接协议，但咖啡店的客户而不是咖啡店的所有者代表实际的“最终用户”。

在未经购买者授权的情况下使用产品或服务的一方（例如黑客/爆竹）通常被视为网络入侵者，而不是“最终用户”本身。

12. 托管中心/托管提供商

托管中心提供各种托管服务，范围包括托管中心运营商提供的利用计算，网络和管理资源进行托管托管，再到托管托管，租户可以提供自己的设备托管在托管运营商机架中。

13. 互联网服务提供商

互联网服务提供商（ISP）是为公众，企业和其他组织提供零售到互联网访问的公司。这些连接可以通过电缆，DSL，卫星，无线，拨号或其他技术进行。互联网服务提供商有时也称为“访问提供商”。

仅为其雇员提供互联网访问权限的企业通常不视为ISP。同样，仅向其他ISP提供批发访问互联网的网络运营商通常会被视为网络服务提供商（NSP），而不是ISP。

14. 恶意软件

“恶意软件”是“恶意软件”的简称。

恶意机器人是恶意软件的一种。其他形式的恶意软件包括以下类别的软件：病毒，特洛伊木马，蠕虫，Rootkit，犯罪软件，击键记录器，拨号程序，间谍软件，广告软件等。区分这些不同类型的恶意软件的重要性并不比理解为什么恶意软件重要。可能会被视为“恶意”。

恶意软件通常会违反以下一项或多项基本原则：

(a) 同意：即使用户没有故意要求进行恶意安装，也可能安装了恶意软件。

(b) 诚实：恶意软件可能假装做一件事，而实际上却在做完全不同的事情。

(c) 尊重隐私：恶意软件可能会侵犯用户的隐私，可能会捕获用户密码或信用卡信息。

(d) 非侵入性：恶意软件可能会通过弹出广告，更改网络浏览器主页，使系统运行缓慢或不稳定并易于崩溃或干扰已经安装的安全软件来惹怒用户。

(e) 无害：恶意软件可能是会伤害用户的软件（如破坏我们系统，发送垃圾邮件或禁用安全软件的软件）。

(f) 尊重用户管理：如果用户尝试删除软件，则可能会重新安装自身或以其他方式覆盖用户首选项。

所有这些加起来就是“软件用户不想要的”。

用户可能会在不知不觉中安装恶意软件，方法是打开通过电子邮件收到的受污染的附件，或者访问包含恶意内容的网页。攻击者针对可能可以远程利用的已知漏洞，或者由用户安装受感染的CD，DVD或拇指驱动器，也可能导致远程攻击者直接感染系统。

15. 缓解

缓解是管理或控制与机器人相关的效果的过程。例如，如果系统感染了垃圾邮件机器人，并散发了不必要的商业电子邮件，缓解措施可能包括过滤从该设备发出的垃圾邮件。

缓解还可能涉及对反射性分布式拒绝服务攻击中使用的设备进行阻止，限制访问或限制服务速率。

请注意，缓解通常不涉及解决基础状况（即“补救”）；缓解只管理与疾病相关的症状。

16. 网络运营商

为有线或无线领域的互联网访问提供网络服务的组织。如果ISP，电信公司，电缆公司和托管提供商提供这些服务，则可能是网络运营商的示例。

17. 通知功能

通知是一个过程，互联网服务提供商与最终用户就机器人恶意软件可能感染最终用户设备或订户如何预防或识别此类感染进行沟通。通知还可能需要一个流程，将最终用户定向到能够自我发现机器人感染的工具。通知可以采用不同的形式，包括ISP向最终用户的直接通知，或通过可用的自我发现工具或第三方的间接通知。通知可以通过多种潜在渠道完成，包括（但不限于）电子邮件，邮政邮件，电话呼叫，浏览器内通知，基于网络的自我发现工具或SMS消息。

18. 预防措施

预防是强化系统或服务，使其较不容易受到破坏和利用的过程。例如，在许多系统上，预防可能涉及：

— 使用可用的安全修补程序修补操作系统和所有应用程序

— **安装或启用防火**墙
— **使用防病毒**软件
— **确保定期**备份系统
— **使用**强密码
— **禁用或阻止**访问不必要的网络服务
— **鼓励用**户安全使用互联网服务（例如，电子邮件，网络浏览等）

19. 反射式分布式拒绝服务攻击

分布式拒绝服务攻击，使用被攻击者的**IP地址**伪造攻击**IP数据包的源地址**，**并将IP数据包**发送到**中**间主机。当中间主机对这些数据包做出响应时，响应数据包将发送到被攻击者的**IP地址**，**用来自中**间主机的流量向被攻击者泛洪。通常在这种类型的攻击中，使用中间主机和协议，其中**响**应数据包大于请求数据包，放大发送给受害者的网络流量。

20. 补救措施

补救是最终用户清理被机器人破坏的计算机，使其不再受到感染的过程。在简单的情况下，这可能涉及安装和运行防病毒产品。在更困难的情况下，修复可能涉及更实质性的干预，直至“裸露”系统（从头开始或至少从最后一次已知的清洁备份格式化和重新安装系统）。系统清洁或重新安装后，通常会经过加固以防止再次感染。

21. 服务器端

网络服务器是一台用于处理请求并将数据通过本地网络或互联网传递到客户端计算机的计算机。数据中心和托管中心中的服务器通常具有与网络的高带宽连接，并且具有大量计算资源，可以在短时间内处理大量请求。

22. 垃圾邮件

不需要和不需要的电子邮件，通常为商业性质，通常以基本上相同的形式发送给大量收件人。垃圾邮件通常由“关联公司”发送，当接收者购买垃圾邮件产品时，这些会员会由运行会员计划的人支付。

II. 感染生命周期：

1. 干净：就互联网服务提供商自愿反僵尸网络行为守则而言，如果计算机或其他网络设备（a）在外部没有明显的感染症状（如发送垃圾邮件，参与分布式攻击，则视为“清洁”）拒绝服务攻击或联系已知的命令和控制主机），以及（b）使用公认的商业或免费/开源反病毒程序对计算机或其他网络设备进行审查（使用最新可用定义）未发现感染，并且（c）计算机

或其他设备，否则在所有方面均正常运行。如果没有相反的证据，则应假定新购买的系统以开箱即用的干净状态启动。

2. 易受攻击：如果计算机或其他网络设备具有一个或多个缺陷或配置错误，使其有可能在拒绝服务或分布式拒绝服务攻击中受到威胁，感染或用作反射媒体，则应视为“漏洞”。易受攻击的设备的常见示例是未打补丁的设备，或使用容易猜测的密码进行访问的设备。请注意，系统可能同时“干净”但“容易受到攻击”，例如在脆弱的系统受到补偿控件（例如防火墙）保护的情况下，即使存在以下情况，也可以避免受到感染或破坏：一个或多个漏洞。

3. 感染：感染的计算机或网络设备是指在未经授权的情况下安装恶意软件或恶意固件的设备。该恶意软件或恶意固件可以称为病毒，特洛伊木马，蠕虫，rootkit，击键记录器，拨号程序，犯罪软件，间谍软件，广告软件等。“恶意软件”可以在FCC CSRIC“互联网服务提供商基础设施”附录A的词汇表中找到。

4. 隔离：感染或受到感染的系统可以隔离，以防止产生不必要的互联网流量。孤立的主机通常被放到“围墙花园”中，在那里只能访问用于补救的一组严格有限的资源，或者只能访问生命安全服务（如用于紧急情况的VoIP电话服务）。

5. 离线：离线系统是指不允许与该主机进行网络访问或从该主机进行网络访问的系统。从概念上讲，可以考虑断开以太网电缆（或禁用以太网交换机端口）的以太网连接主机，尽管在电缆调制解调器连接，DSL方面使用明显不同的技术过程连接，无线访问，调制解调器访问等。

6. 消毒：当系统被感染后恢复到“干净”状态（如上定义）时，应视为“已消毒”。消毒系统的第一步通常是安装和运行防病毒产品（如果尚未安装和更新）。在某些情况下，可能有必要从头开始格式化和重新安装系统，以克服特别隐蔽的持久性恶意软件。

7. 强化：强化系统是经过系统配置以消除系统漏洞（或潜在漏洞）的系统。例如，除其他事项外，硬化系统将进行最新修补，禁用所有不必要的服务，需要对所有敏感网络流量进行加密，将使用强 密码或多因素身份验证，将安全记录到系统外记录主机等。

8. 重新感染：已消毒但未硬化的系统通常会迅速被重新感染。

9. 折衷方案：虽然许多易受攻击的系统可能因感染恶意软件而受到攻击，但其他易受攻击的系统也可能由于弱口令或错误配置（例如未经授权方无意间能够修改的关键文件）而受到损害。遭到破坏的系统是不可信的。

10. 托管：“托管主机”是集中管理的主机，而不是自我托管的主机，由系统用户管理。托管主机通常在大型公司和政府机构中使用。

11. 受监控的：受监控的主机会不断（或至少定期）检查异常网络流量或对关键系统文件的未经授权更改。监控可以通过网络安全系统（如Snort）或通过基于主机的系统（如Tripwire）进行。

12. 更换：虽然大多数用户都试图对感染的系统进行消毒和加固，但有些用户可以选择更换新系统。然后，可以将先前的系统出售给第三方，第三方可以将系统与安装在系统上的任何恶意软件一起获取。

13. 共享：一个共享系统是由多个人使用的系统。共享设备的常见示例是父母或父母以及孩子或其他家庭成员使用的家庭设备。与仅由一个实体使用的系统相比，共享设备似乎更容易受到感染（或其他安全问题）。

14. 孤立的：孤立的设备或程序是一个较旧的设备，供应商不再为此发布关键的安全/稳定补丁。孤立的系统或程序通常无法进行加固。

III. 生态系统角色

1. 客户：在ISP的ABC中，指为互联网服务付费的ISP。

2. 系统所有者：拥有给定计算机或其他设备的人。

3. 系统用户：系统所有者有意允许使用计算机或其他设备的人。

4. 支持人员：对于家用计算机，支持人员可以是帮助系统所有者或用户使用和维护计算机的家庭成员或朋友。支持人员也可以是计算机所有者或用户为此目的雇用的商业计算机支持专家。

5. 互联网服务提供商（ISP）安全/滥用团队：处理与客户投诉有关的个人或团体。

6. 供应商：制造和销售计算机系统或软件程序的公司。例如，您可能会谈论操作系统供应商，应用程序软件供应商，硬件供应商或防病毒软件供应商。

7. 执法：警察，警长，联邦代理人或其他宣誓就职的个人，有权调查犯罪，收集证据和逮捕。

8. 监管机构：负责管理业务实践或其他活动以确保基本公平或监管合规的州或联邦官员。监管机构的一个例子是美国联邦贸易委员会。监管机构通常采用民事制裁（如行政罚款或民事诉讼），而不是刑事制裁（如逮捕/监禁）。

9. 未经授权的用户：无意使用计算机或其他设备的人，系统所有者或使用超出授权范围的授权访问权限的人的权限。

10. 恶意软件作者：设计和编码恶意软件（如机器人）的程序员或编程团队。

11. 僵尸僵尸：僵尸僵尸是指操作被僵尸计算机网络的人，通常使用这些计算机发送垃圾邮件或攻击其他计算机。僵尸机器人通常通过命令和控制主机（例如，受其控制的服务器）向“其”机器人发送命令。

12. 会员：在这种情况下，会员是指帮助营销特定产品或服务以换取补偿的人，通常使用按展示次数付费，按点击付费，按安装付费或收益分享模型：

(a) 每次展示付费（PPI）：会员通常是网站所有者，根据向访问者展示网站横幅或其他广告的次数付费

(b) 每次点击付费：在这种模式下，当用户实际点击广告时向联盟会员付款

(c) 每次安装付费：在这种模式下，为会员提供的程序秘密或在用户知情的情况下（如果是程序的“赞助访问”报价的一部分）安装在新系统上时，向会员支付费用或原本需要购买的网站）

(d) 收益分享：在这种模式下，联盟会员将获得与其推荐客户相关的销售额的一定百分比。

13. 列表卖家：列表卖家是指编辑和分发电子邮件地址列表的人。例如，想要向非法的在线赌场发送垃圾邮件的垃圾邮件发送者可以购买已知与在线赌徒相关的电子邮件地址列表。

14. 防弹托管公司：所谓的防弹托管公司是指同意托管网站或其他在线存在的公司，尽管该活动可能引起投诉，但通常以交换被托管方支付溢价的形式交换。子弹证明托管公司可用于托管垃圾邮件网站，恶意软件，虐待儿童资料或其他常规托管公司可能无法接受的其他内容。

15. 防弹域名注册机构：所谓的防弹域名注册机构是指允许垃圾邮件发送者或其他网络罪犯注册域名并保持该域名正常运行的机构，尽管可能存在与该域名相关的投诉。通常以高于市场域名注册费的价格提供这项服务。

16. 付款处理器：会员销售时，通常使用信用卡付款。处理信用卡交易的实体称为“支付处理器”。

17. 托运人：托运人是管理会员计划订单履行的实体。例如，专门从事非法药品的直接托运人可以打包和发送由垃圾邮件发送者获得的订单。

18. 在线货币兑换商：某些会员可以使用在线货币支付，而不是通过邮寄支票或直接存款支付。在线货币兑换器使某些人可以购买在线货币换取现金，反之亦然。

19. 滥用情况报告者：第三方向ISP或通过信息交换中心（如计算机安全事件响应小组）报告滥用事件。

附录C：分布式拒绝服务攻击分类

1 分布式拒绝服务攻击-攻击可用性

1.1 分布式拒绝服务攻击的定义

为进行分析，工作组使用了以下定义的分布式拒绝服务攻击：“拒绝服务（DoS）或分布式拒绝服务（DDoS）攻击是为了阻止合法用户访问信息。或服务（美国CERT）。”分布式拒绝服务攻击由两个或多个同时攻击同一目标的系统或攻击者组成。[25]

1.2 1.2分布式拒绝服务攻击目标

1.2.1 攻击容量

1.2.2 攻击国家

1.3 分布式拒绝服务攻击工具

1.3.1 僵尸网络

1.3.1.1 客户端僵尸网络

1.3.1.2 服务器僵尸网络

1.3.1.3 参与式僵尸网络

1.3.1.4 其他僵尸网络

1.3.2 攻击线束

1.3.3 流量生成应用程序

2 IPv4和IPv6分布式拒绝服务攻击

2.1 容量分布式拒绝服务攻击

2.1.1 直接数据包泛洪

2.1.1.1 ICMP和ICMPv6

2.1.1.2 UDP协议

2.1.1.3 TCP

2.1.1.3.1 SYN洪水

2.1.1.3.2 RST洪水

2.1.1.3.3 ACK洪水

2.1.1.3.4 RST洪水

2.1.1.3.5 空洪水

2.1.1.3.6 SYN / ACK泛洪

2.1.1.3.7 XMAS-树洪水

2.1.1.3.8 无效的标志组合洪水

2.1.1.3.9 端口0洪水

2.1.1.4 碎片数据包

2.1.1.4.1 UDP协议

2.1.1.4.2 TCP

2.1.1.5 协议0

2.1.1.6 GRE（通用路由封装）泛洪

2.1.1.7 ESP（IPsec封装安全有效载荷）泛洪

2.1.1.8 RTP泛洪

2.1.1.9 其他“非标准”协议泛滥成灾

2.1.2 反射/放大

2.1.2.1 UDP反射/放大

2.1.2 反射/放大

2.1.2.1 UDP反射/放大

[25] http://www.us-cert.gov/ncas/tips/ST04-015

2.1.2.1.1 域名系统反射/放大
2.1.2.1.1.1 使用开放式域名系统（DNS）递归器和权威服务器的域名系统（DNS）反射/放大
2.1.2.1.1.2 仅使用权威服务器的域名系统反射/放大
2.1.2.1.2 SNMP反射/放大
2.1.2.1.3 NTP反射/放大
2.1.2.1.4 电荷反射/放大
2.1.2.1.5 TFTP反射/放大
2.1.2.1.6 RADIUS反射/放大
2.1.2.1.7 SIP反射/放大
2.1.2.1.8 其他UDP反射/放大攻击
2.1.2.2 TCP反射/放大
2.1.2.2.1 SYN / ACK反射
2.1.2.2.2 RST反射
2.2 应用层分布式拒绝服务攻击
2.2.1 HTTP
2.2.1.1 获取
2.2.1.2 开机自检
2.2.1.3 CGI
2.2.1.4 “慢速” HTTP变体
2.2.2 SSL / TLS
2.2.2.1格式错误的SSL / TLS
2.2.2.2 SSL / TLS协商
2.2.2.3 HTTP / S封装攻击
2.2.3 域名系统
2.2.3.1 权威域名系统（DNS）请求泛洪
2.2.3.2 递归域名系统（DNS）请求泛洪
2.2.3.3 权威区域委托攻击
2.3.4 SIP
2.2.4.1 邀请洪水
2.2.4.2 信息洪水
2.2.4.3 通知洪水
2.2.4.4 重新邀请洪水
2.3.5 ssh
2.2.5.1 SSH协商
2.2.5.2 登录暴力破解
2.3.6 中层和后层应用程序
2.2.6.1 AAA子系统
2.2.6.2 数据库
2.2.6.3 图像生成系统
2.2.6.4 其他中层和后层应用程序2.2.7其他应用程序
2.3 状态耗尽分布式拒绝服务攻击

附录D：分布式拒绝服务攻击缓解案例研究

ISP亚组案例研究

I. 背景资料

互联网服务提供商（ISP）多年来一直积极缓解分布式拒绝服务（DDoS）。在最常见的早期攻击形式中，连接到家庭宽带服务的个人计算机开始遭受恶意软件感染，这会将机器转变为所谓的僵尸（现在称为僵尸机器人）。攻击者使用分别受损的服务器进行控制，然后可以命令大批机器人在某个受害者（通常是网站）上发送大量数据。这样，网站将变得不堪重负，无法处理正常的授权请求。*26*

从大约1999年到2011年，针对大多数ISP基础设施的数据量以及对手制作数据量的技能均处于可管理的阈值内。在过去的十二年里，针对大型互联网服务提供商基础设施的任何部分，发生的影响服务的攻击几乎没有。包括对主要第1层ISP域名服务基础设施的攻击。在此期间，攻击规模通常在每秒千兆位范围内。

此外，在同一时期，一些互联网服务提供商（ISP）为企业客户开发了新的托管安全服务 ，以帮助缓解其基础设施上的分布式拒绝服务攻击。几个 美国金融机构目前订阅这些服务，通常涉及基于容量或基于应用程序的解决方案实时检测攻击。例如，可以使用数据收集工具根据流量峰值定量检测分布式拒绝服务攻击，然后使用边界网关协议（BGP）将流量重定向到专门设计的过滤攻击的防火墙。然后，经过清理的流量会通过ISP的基础设施“隧道传输”到客户站点。

在2012年末，互联网服务提供商开始看到规模更大的攻击，攻击者会创建足够的入站流量，潜在地淹没某些互联网服务提供商洗涤基础设施的入口容量。
此外，触发攻击的僵尸网络很独特，因为它通常利用相当大的网络连接上的服务器为僵尸机器人，而不是消费宽带连接上的受损个人电脑。在第三季度末，同一对手在银行网站上发起了一系列“电报攻击”，并在pastebin上定期发布警告。这些攻击达到前所未有的规模，通常再次针对域名系统。作为响应，互联网服务提供商（ISP）实时进行了一些调整，以增强其基础设施，清理平台和域名系统（DNS）站点容量。*27*

本案例研究旨在为互联网服务提供商提供解释和建议的做法应对未来的大规模分布式拒绝服务攻击。

26拒绝服务（DoS）或分布式拒绝服务（DDoS）攻击是试图阻止合法用户访问信息或服务26（US-CERT）。

27这是流量工程的持续过程。许多ISP持续监控流量，以确保足够的容量。此过程适用于到ISP分布式拒绝服务清理基础设施的数据链接。

II. ISP分布式拒绝服务攻击的简化分类法

虽然更广泛的工作组已经制定了详细的分布式拒绝服务攻击分类法，但互联网服务提供商（ISP）小组认为有必要开发一个简化版本以用于案例研究。该小组还讨论了将分布式拒绝服务攻击分为两个维度的模型：

1. 攻击类型-容量攻击或应用程序攻击
2. 攻击方向-北向南或东向西。
    a. *北向南是源自ISP网络外部的攻击，针对ISP客户或ISP网络内部的基础设施。*
    b. *南北攻击是源自ISP网络内部的攻击，针对ISP网络内部的外部实体或基础设施。*
    c. *东西方代表发起于客户并针对另一客户的攻击*

范例：

1. 客户或互联网服务提供商（ISP）基础设施受到外界的打击（南北向）
2. 越野车客户泛滥ISP DNS服务器的客户-南北
3. 客户将数据包泛洪到外部目标-南北
4. 客户互相攻击-从东到西

该分组建议，将相互攻击的客户与攻击基础设施或外部目标的客户分开，因为有时需要不同的检测和缓解策略。例如，如果同一地区的两个客户相互攻击，流量可能不会越过ISP收集流量数据的任何路由器，也不会撞到ISP对等边缘的清理中心。

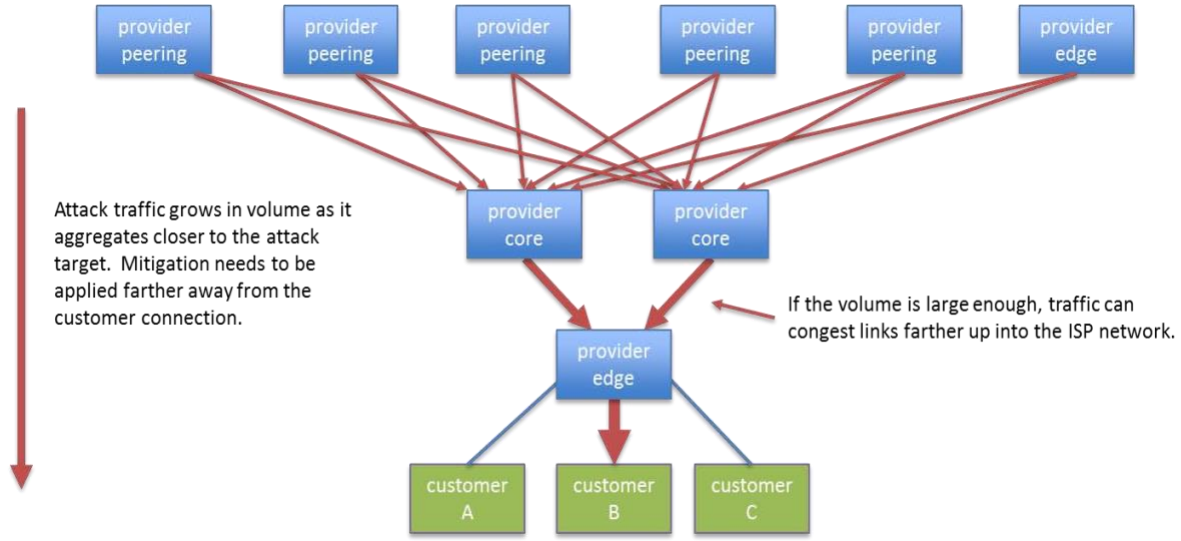
III. ISP遭受的示例分布式拒绝服务攻击

A. 针对大客户的基于服务器的容量式拒绝服务攻击

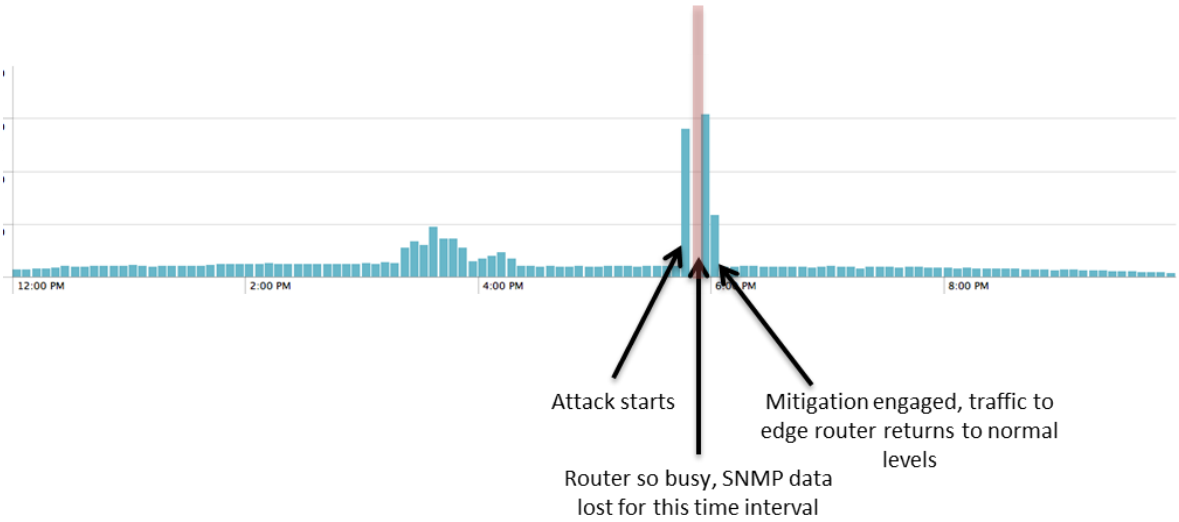
背景信息：此攻击使用大容量UDP / 80数据包（垃圾流量）耗尽目标带宽。攻击大约用了10分钟，达到峰值流量超过70Gbp s。当时，这是ISP网络上最大的攻击之一。攻击IP数以千计。

缓解步骤：

1. 客户的拒绝服务检测服务可以识别攻击和目标IP。
2. 客户使用了拒绝服务缓解服务，流量被重新路由到了拒绝服务缓解中心。攻击流量被丢弃，合法流量被传递。



如果攻击规模较大（10s至100s Gbps），则可能对非攻击目标客户造成附带影响。如果能够迅速发现并缓解攻击，通常可以避免附带损害。



建议做法：

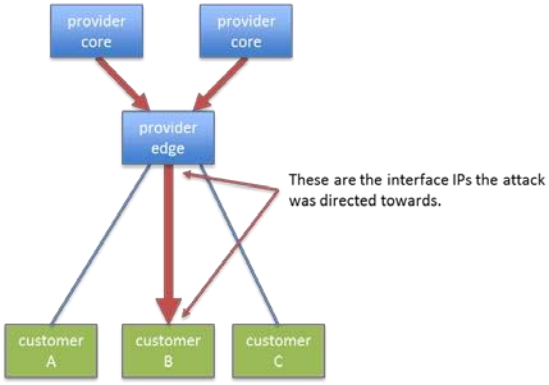
1. 如果攻击没有订阅任何拒绝服务缓解服务的客户，则应在ISP路由器上配置黑洞路由。
2. 基于SNMP轮询，网络流量，探测器或类似技术的网络检测和警报对于快速检测带宽饱和问题（15分钟或更短）至关重要。
3. 应部署Netflow收集或某种类似技术来识别攻击目标和目标协议。
4. 提供攻击缓解/清理服务的提供商应设计基础设施这样攻击流量不会集中在单个区域或清理中心。这些中心的能力应适当调整规模。

B. 针对ISP和客户基础设施IP的攻击

背景信息：此次攻击再次使用大容量UDP / 80数据包（垃圾流量）耗尽目标带宽。但是，在这种情况下，攻击首先针对客户的路由器接口IP，然后针对ISP。

缓解步骤：

1. 通过网络流识别攻击和目标IP。
2. ISP和客户之间的/ 30子网被黑了。
3. 随后，在ISP边界路由器上应用了过滤器，以限制发往ISP基础设施的流量。



建议做法：

- 尽可能通过过滤或路由将流量限制到ISP点对点基础设施。
- 请勿使用点对点基础设施IP进行NAT，隧道终止或其他需要传播和路由IP的流量（否则将不需要）。
- 按照案例研究1的建议实施检测，以便快速识别这些攻击。请注意，当以ISP地址为攻击目标时，客户将永远看不到流量。

潜在挑战：

- 在每个ISP入口点进行过滤可能是不切实际的。
- 将网络重新寻址到未路由的空间可能是一项困难且耗时的任务。

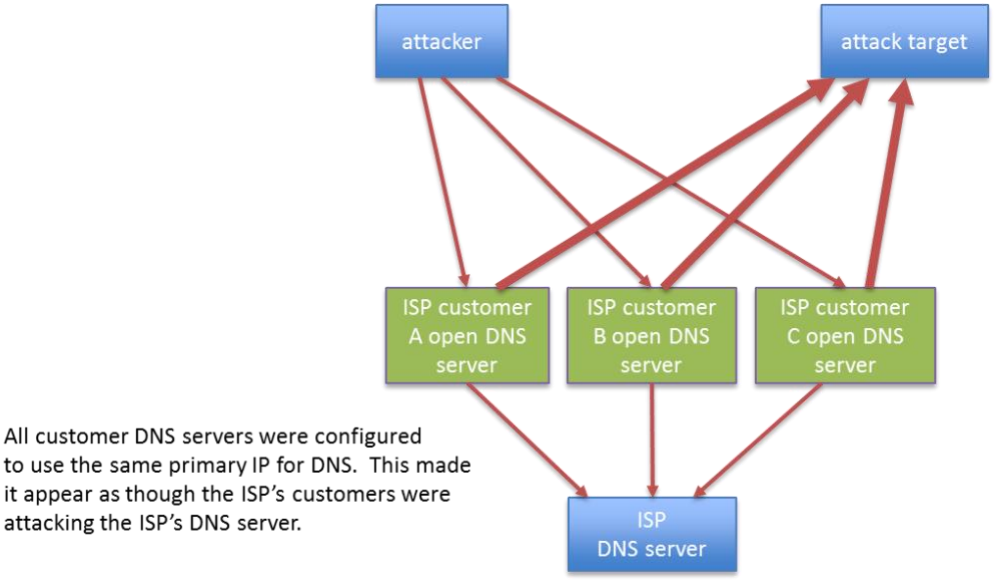
C. 域名系统反射攻击造成的附带损害

背景信息：此次攻击再次使用大量欺骗UDP /53数据包（域名系统（DNS）查询）流向未经过滤的递归域名系统（DNS）服务器，放大攻击并耗尽目标带宽。在这种情况下，即使攻击根本不是针对ISP的，ISP也有遭受不利影响的风险。

缓解步骤：

1. 通过网络流以及在域名系统（DNS）服务器上配置的日志记录，识别出攻击以及目标IP。
2. 来自客户的查询通过拒绝服务缓解服务进行路由。

3. 互联网服务提供商（ISP）随后采取后续行动，对客户设备进行适当过滤。



建议做法：

- 为关键基础设施（如域名系统服务）配置攻击缓解服务。缓解措施的示例包括流量清理和服务速率限制。
- 根据基础设施服务的需求扩展缓解能力。
- 尽可能使用任播或内容分发网络等技术分发关键服务。
- 为关键基础设施提供带外管理，以使攻击不会阻止对缓解攻击所需设备的访问。
- 将服务的公开范围限制为仅需要访问它们的服务（例如，DNS，NTP等）。
- 避免使用配置了未保护服务的设备，例如未过滤的域名系统和已知的SNMP社区字符串。
- 在可行的情况下（例如，住宅网络和托管中心）应用反欺骗控件。

潜在挑战：

- 部署缓解能力可能与攻击者"军备竞赛"。
- 在没有不可接受的附带影响的情况下，无法有效过滤某些服务。
- 对于许多中转客户来说，不可能采用反欺骗技术（BCP 38）。

D. 家庭网关/路由器发起的分布式拒绝服务

- **背景：** 某个特定的家庭网关供应商存在一个错误，导致其泛洪域名系统（DNS）前面的调制解调器重新引导时以线速请求。互联网服务提供商（ISP）在其最大的市场中提高了宽带速度，需要重启调制解调器。大约有250个家庭网关开始泛洪域名系统（DNS）请求，关闭了ISP的域名系统（DNS）集群
-
- **发现的问题：**

- 没有深入到ISP网络的DDOS缓解功能。数据清理中心位于ISP网络的对等边缘。

- 域名系统（DNS）服务器每次回复都返回其他可选的授权信息，从而放大效应
- ISP的负载平衡器未使用速率限制功能
- 互联网服务提供商（ISP）很难通过查询接口管理域名系统（DNS）服务器，宽带宽带域名系统（DNS）泛洪使查询服务器饱和。

- **缓解步骤：**

1. 用于捕获DNS数据包的带外安全工具。配置了工具，计算给定时间段内看到的数据包数量，并对超过这些阈值的客户生成警报。
2. 将警报投放到现有的滥用管理系统中，并使客户离线
3. 自动化流程以备将来使用

建议：

- 对于任何给定的服务，请确保返回的信息尽可能少，以免轻易用作放大器。
- 通过将管理接口与服务接口分开，确保服务器在受到攻击时仍可访问。
- 利用现有网络硬件中可用的安全功能（如速率限制）。
- 缓解可以使用被动监控器脱离信号完成，该监控器向其他工具发出信号通知采取某种措施。

E. 空路由

背景：空路由是DDOS缓解的最简单形式，也是附带损害最大的一种。丢弃发往给定IP地址的所有流量，真是一锤定音。

优点：

- 实施简单快捷
- 在最大链路上丢弃网络对等边缘的流量

缺点：

- 将所有流量都丢弃到给定的IP，而不仅仅是恶意流量

用例：

- 住宅（或其他动态IP）客户受到攻击。
  ISP可以简单地丢弃发往目标IP的所有流量，并为客户提供新流量
- 出站攻击。如果另一个ISP的IP地址受到攻击，并且该ISP指示客户没有合法需要到达该地址，则第一个ISP可以在数据包离开网络之前丢弃数据包。例如：另一台ISP的路由器受到攻击。首批ISP的客户没有理由直接向该路由器发送数据包，因此在我们的网络上将其IP路由为零。

IV. ISP缓解技术（工具/技术控制）

响应分布式拒绝服务攻击有两个主要阶段：

阶段1：检测

互联网服务提供商可以使用基于容量的或基于应用程序的方法检测分布式拒绝服务攻击。例如，在基于容量的解决方案中，互联网服务提供商（ISP）将建立基准，可以确定攻击流量异常。检测攻击的另一种方法是直接来自客户，客户通常自己观察入口流量的逐渐增加，并会相应地与ISP联系。

检测：

类型	南北	南北	东西
容量	基于Netflow的解决方案 高效监控 受害者打来的电话	基于Netflow的解决方案 受害者打来的电话	受害者打来的电话
应用程序	基于DPI的解决方案 基于主机的解决方案 受害者打来的电话	基于DPI的解决方案 基于主机的解决方案 受害者打来的电话	受害者打来的电话

阶段2：缓解

DDOS响应活动的缓解阶段的目标是抵抗恶意行为的影响。缓解通常采用以下两种形式：（1）过滤不良流量，或者（2）通过降低僵尸网络源来降低攻击强度。第二种措施可以通过多种方式完成，例如在攻击之前，期间和之后联系受感染的计算机和服务器的所有者。因此，ISP分布式拒绝服务安全活动的主要目标涉及成功阻止，转移，过滤和减慢针对受害者站点的正常入口流量中嵌入的攻击流量的所有可能尝试。由于大多数DDOS攻击差异很大（与最近的银行攻击相比，常规节奏有所不同），因此决策过程可能是高度动态的，并且通常依赖于实时分析。

缓解措施：

一般来说，通常会首选能够解决问题的最简单的缓解技术。但是，从服务角度来看，更钝化技术和对合法流量影响更大的技术是更具体的缓解技术。如前所述，在给定情况下的适当操作确实取决于攻击和目标的具体情况。

如果服务或客户受到黑洞攻击，则首选黑洞路由

28应用层分布式拒绝服务攻击可能比传统的基于容量的工具（如深度数据包检测）的使用更难以检测，在某些情况下可能需要更多的侵入性工具，并且由于使用SSL或其他基于加密的攻击而变得复杂。

攻击不会丢失所有流向目标的流量，不会造成任何性能下降或中断。例如，在目标地址永远不需要接收来自互联网的任何流量的情况下，该IP的黑洞路由是最简单的答案。此外，还可以通过黑洞路由攻击目标来缓解出站攻击。如果目标地址需要服务，但攻击使用不同的协议或服务，则路由器ACL等数据包过滤器可能有效。非平凡的容量攻击（针对所需服务）通常需要更专业的清理服务或DPI解决方案。这些服务旨在允许大多数合法流量通过，同时阻止大多数攻击流量。

类型	南北	南北	东西
容量	擦洗中心/地毯 黑洞路线 路由器访问控制列表 BGP Flowspec	暂停攻击者的服务 其他设备控制，例如阻止变频器上的端口 黑洞路线 路由器访问控制列表	暂停攻击者的服务 其他设备控制，例如阻止变频器上的端口 黑洞路线 路由器访问控制列表
应用程序	擦洗中心/地毯 基于DPI的解决方案 基于主机的解决方案	基于DPI的解决方案 基于主机的解决方案 暂停攻击者的服务 其他设备控制，例如阻止串口上的端口	暂停攻击者的服务 其他设备控制，例如阻止变频器上的端口 基于主机的解决方案

V. 其他

- 鉴于许多分布式拒绝服务攻击源于受感染的最终用户，互联网服务提供商（ISPs）审查了互联网服务提供商基础设施（ABC）一套由CSRIC III于2012年发布的缓解恶意软件的建议。
- 在滥用服务台和通知流程方面，可以为托管服务提供商开发类似的最佳实践，在受到基于数据中心攻击的情况下向托管中心受感染的租户发出警报。
- 互联网服务提供商（ISP）审查了BCP 38和其他可能管理IP地址欺骗的替代方法。

金融子群体案例研究

案例研究：

从2012年下半年到2013年中，美国金融机构（USFIs）遭受持续不断的对其网络的分布式拒绝服务（DDoS）攻击。分析表明，其中一些攻击来自民族国家威胁行为者。这些攻击显示了预先计划的证据，而且复杂性还在不断发展。

可以相信，对USFIs的分布式拒绝服务攻击是更大的攻击策略的一部分，预示着更严重的攻击。目标的美国金融机构代表美国经济活动的重要组成部分，象征美国经济稳定，如果妥协，可能对金融部门构成系统性风险。声称拥有信用的组织威胁要发起更多攻击。

什么是DDOS攻击？
分布式拒绝服务攻击是一种协作式网络攻击，旨在通过消耗网络带宽或通过来自多个自治源的同时数据连接使目标系统不堪重负，破坏信息处理系统或应用程序的可用性。分布式模型催生了僵尸网络，僵尸网络是恶意软件感染主机的集合，能够按对手的意愿发动分布式拒绝服务攻击，而攻击者可以控制它们显着改变攻击速度。

使用的分布式拒绝服务类型：

- UDP泛洪
- TCP泛洪
- 搜索功能攻击
- 大文件GET
- 基础设施级别的攻击
- 认证门户攻击

攻击步骤：

- 端口80 SYN如果可能的话，用一些UDP淹没网络带宽。
- 使用格式错误的UDP / TCP数据包攻击域名系统（DNS）服务器。
- 攻击网络服务器上的域名系统（DNS）端口。
- 攻击SSL连接。
- URL（最新策略）从主站点切换到辅助站点。
- HTTP / HTTPS后攻击（搜索功能）。
- 端口80/443/53

工具：

- 攻击者使用自定义攻击脚本将流量发送到端口80、443、53、1800

自适应技术：

- 大量（带宽/数据包）恒定变形（端口/协议）。

- 动态定制攻击以缓解攻击。
- 能够破坏并利用具有高带宽连接的恶意软件感染服务器。
- 能够添加到僵尸机器人和添加新客户端来规避IP过滤器/黑名单。

虽然2012/13年度的攻击主要集中在带宽攻击上（第3层和第4层）；威胁行为者转移并发展了能力，以进行更复杂的第7层攻击。威胁行为者使用SSL进行攻击设计，使攻击流量看起来像合法流量，目的是伪装其邪恶活动和愚蠢的网络防御。此外，攻击已从单一目标演变为同时或快速连续攻击多个USFI，其中攻击者在目标上"驻留"数小时或数天。

技术控制：

1. 运营商协议速率限制
2. 载波源IP阻塞
3. 目的地IP地址或协议的运营商黑洞过滤
4. 使用自定义脚本进行负载平衡器过滤
5. 本地网络应用程序防火墙
6. 第三方基于BGP的数据清理
7. 第三方基于域名系统的数据清理
8. IPS规则
9. 基于第3层或第4层特征的网络块
10. 本地分布式拒绝服务检测/缓解设备
11. 基于源IP地理位置的运营商阻塞
13.连接速率限制
15. 本地数据包/会话生存时间（TTL）过滤
16. 本地协议/端口过滤

新兴趋势

- 僵尸网络架构变得越来越复杂，更难追踪，C2（命令和控制）系统越来越多地使用代理服务器混淆执行命令的系统位置。
- 设备在全球范围内越来越分散，由于各国法律通常不同，有时甚至相互矛盾，因此很难协调关闭这些系统。
- 僵尸网络日趋复杂，其中一些能够在完成攻击后擦除受感染系统的整个硬盘。
- 分布式拒绝服务工具将/将继续变得更加复杂，具有多任务和多线程功能，有可能同时对多个目标和服务发起攻击。
- Twitter等社交媒体可能会被用来重定向和配置僵尸，将其作为新的攻击手段。
- 随着移动设备的激增，攻击者将入侵并安装僵尸网络，并利用其进行分布式拒绝服务攻击。
- 攻击者已经开发出能够主动监控防御动作并不断调整攻击以击败缓解攻击的能力。攻击者已经证明可以添加机器人，添加新客户端来逃避IP过滤器/黑名单。

互联网安全专家小组研究

案例研究1：互联网数据中心（IDC）中的服务器发起的出站/交叉分布式拒绝服务攻击

IDC服务器由于软件版本易受攻击而受到危害；没有根，没有欺骗流量。

- 多个不断变化的攻击媒介– HTTP，HTTP /S，格式错误的域名系统（DNS）查询洪水；通过HTTP和HTTP /S进行的GET消耗目标网络上的出站传输带宽。对合法服务器用户，IDC运营商，中转网络运营商的附带影响。

- 每个源每秒高数据包（pps）/每秒比特（bps）

案例研究2：利用开放域名系统递归的域名系统反射/放大攻击。

攻击者欺骗攻击目标的IP地址，将对预先识别的大域名系统记录（Any记录，大TXT记录等）的域名系统查询发送到滥用的开放域名系统递归服务器，或直接发送到权威域名系统（DNS）服务器。

攻击者使用DNS选择他要定位的UDP端口，通常仅限于UDP / 53或UDP / 1024-65535。目的端口是UDP / 53

服务器直接“响应”攻击目标或具有较大域名系统响应的中间开放式域名系统递归服务器。在攻击目标中，未经请求的域名系统响应流会分解为初始和非初始碎片。

响应大小通常为4096 – 8192字节（可以更大或更小），分为多个碎片。

由于流行的以太网MTU，攻击目标收到的数据包大小通常约为1500个字节，而且很多。

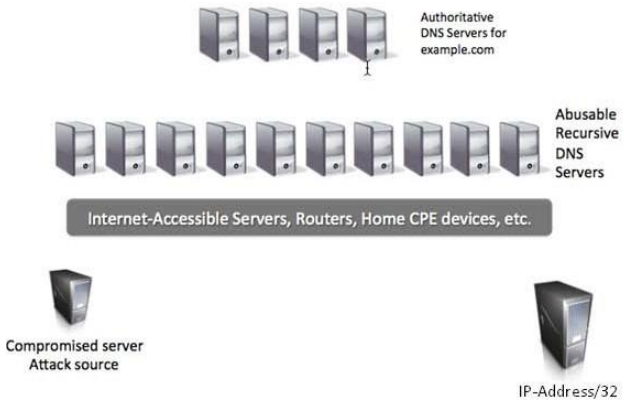
随着这些分散的域名系统（DNS）响应流汇聚在一起，攻击量可能会很大-迄今为止，经过验证的此类攻击最大规模约为200GB /秒。 100GB /秒的攻击很普遍。

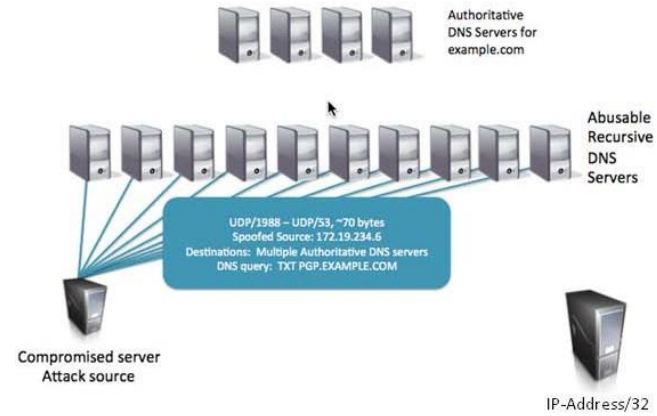
目标的互联网传输带宽，目标的同级/上游的核心带宽以及被滥用的各种域名系统（DNS）服务与目标之间的中间网络的核心带宽已饱和。

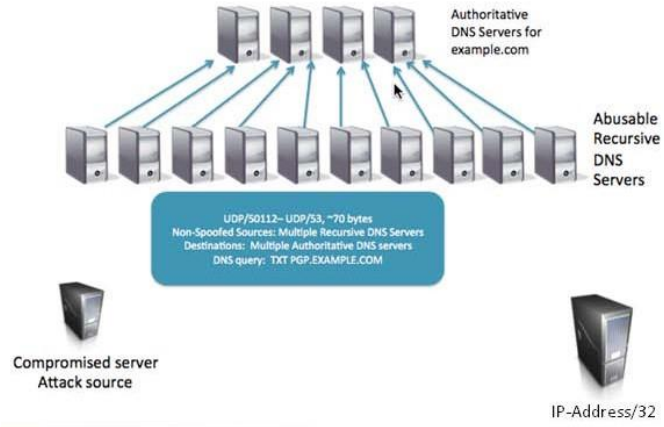
在大多数涉及中间开放域名系统递归服务器的攻击中，反射器是
攻击者可以利用约20,000 – 30,000滥用递归域名系统（DNS）。在某些攻击中，观察到多达50,000台可滥用的开放递归域名系统（DNS）服务器。

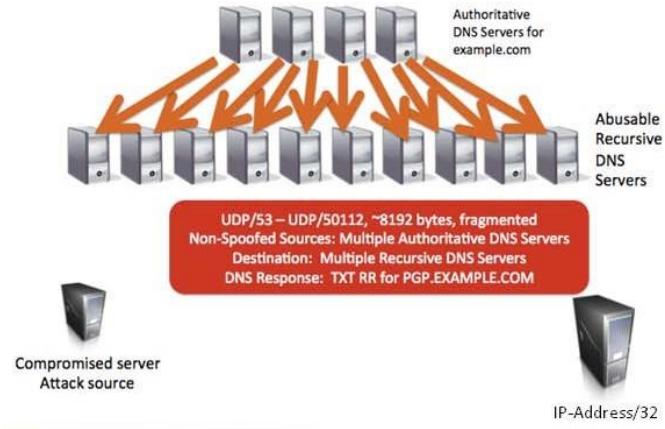
在直接利用权威域名系统（DNS）服务器的攻击中，攻击者可能利用成百上千的此类服务器。

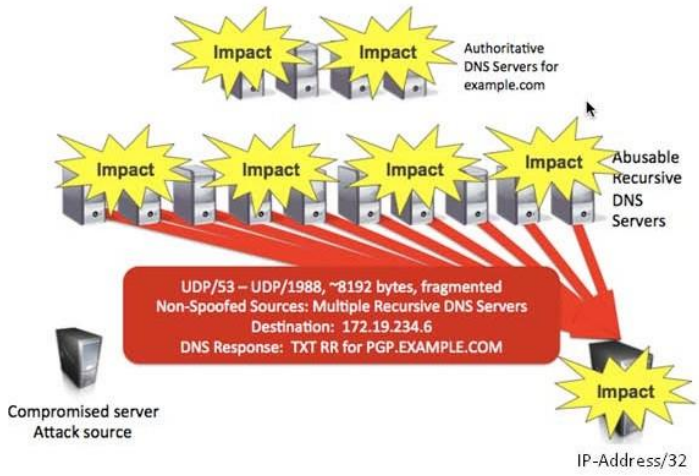
许多公知的权威域名系统（DNS）服务器是任播的，在互联网上部署多个实例。






Authoritative
DNS Servers for
example.com
Abusable
Recursive
DNS
Servers
UDP/50112– UDP/53, ~70 bytes
Non-Spoofed Sources: Multiple Recursive DNS Servers
Destinations: Multiple Authoritative DNS servers
DNS query: TXT PGP.EXAMPLE.COM
Compromised server
Attack source
IP-Address/32


Authoritative
DNS Servers for
example.com
Abusable
Recursive
DNS
Servers
UDP/53 – UDP/50112, ~8192 bytes, fragmented
Non-Spoofed Sources: Multiple Authoritative DNS Servers
Destination: Multiple Recursive DNS Servers
DNS Response: TXT RR for PGP.EXAMPLE.COM
Compromised server
Attack source
IP-Address/32



案例研究3：受到ntp反射/放大攻击的终端企业网络Web服务器。

攻击者欺骗攻击目标的IP地址，向运行在服务器，路由器，家用CPE设备等上的多个滥用NTP服务发送单播列表，showpeers或其他NTP级别6 / -7管理查询。

攻击者选择他想要定位的UDP端口（通常为UDP / 80或UDP / 123，但可以是攻击者选择的任何端口），并将其用作源端口。目的端口是UDP / 123。

NTP服务使用从UDP 123到目标的约468字节数据包的非欺骗流“回复”攻击目标；目标/端口是攻击者在生成NTP monlist / showpeers / etc时选择的源端口。查询。

随着这些多个非欺骗NTP回复流的融合，攻击量可能会很大。–迄今为止，此类验证的最大攻击速度超过400GB /秒。 100GB /秒的攻击很普遍。

由于攻击量巨大，目标的互联网传输带宽，目标的对等/上游的核心带宽以及被滥用的各种NTP服务与目标之间的中间网络的核心带宽会因非欺骗攻击流量。

在大多数攻击中，攻击者利用约4,000至7,000之间的可用NTP服务。在某些攻击中，最多观察到50,000个NTP服务。

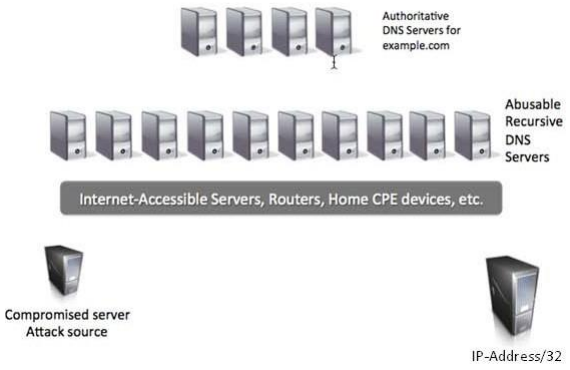
服务器，服务，应用程序，互联网访问等。等在目标网络上，大量流量（数十或数百GB /秒）不堪重负，无法使用。

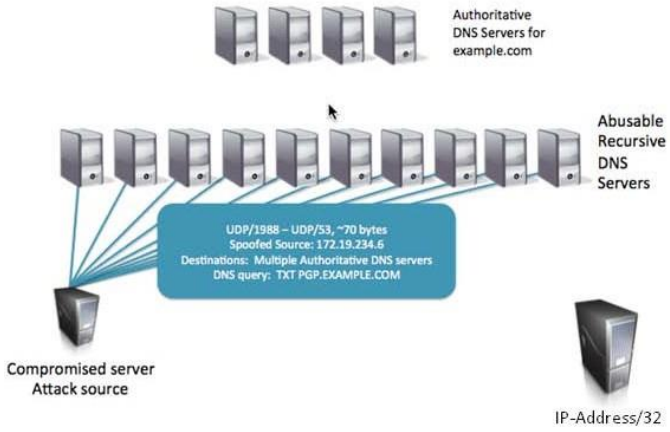
目标网络的对等链路/传输链路完全饱和。

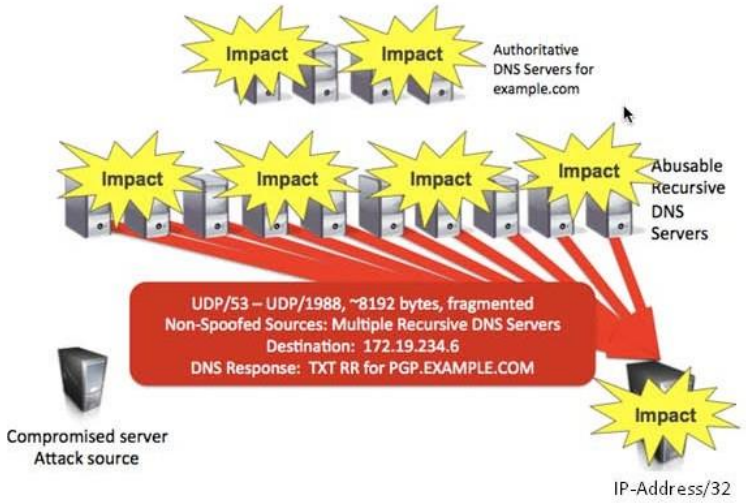
NTP反射器/放大器和目标网络之间的中间网络对等链路/传输链路/核心链路的总饱和或接近全部饱和，包括目标网络的直接对等体/传输提供商的网络

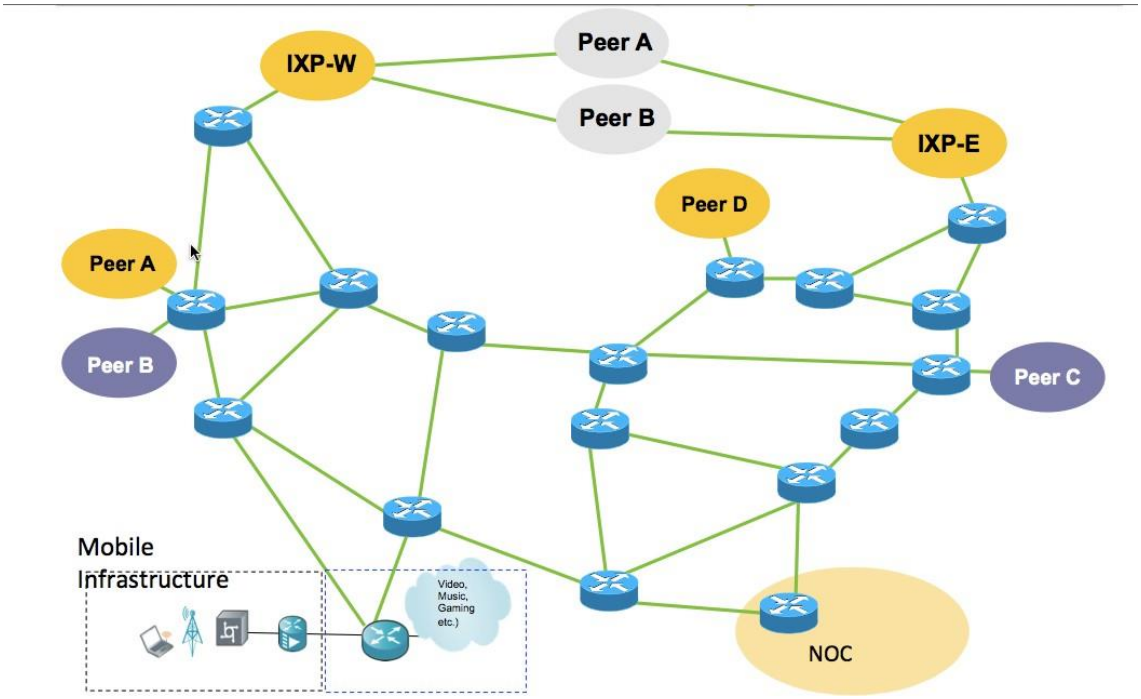
广泛的附带损害–
数据包丢失，延迟，非参与方的互联网流量高延迟，恰好穿越了这些攻击所饱和的网络。

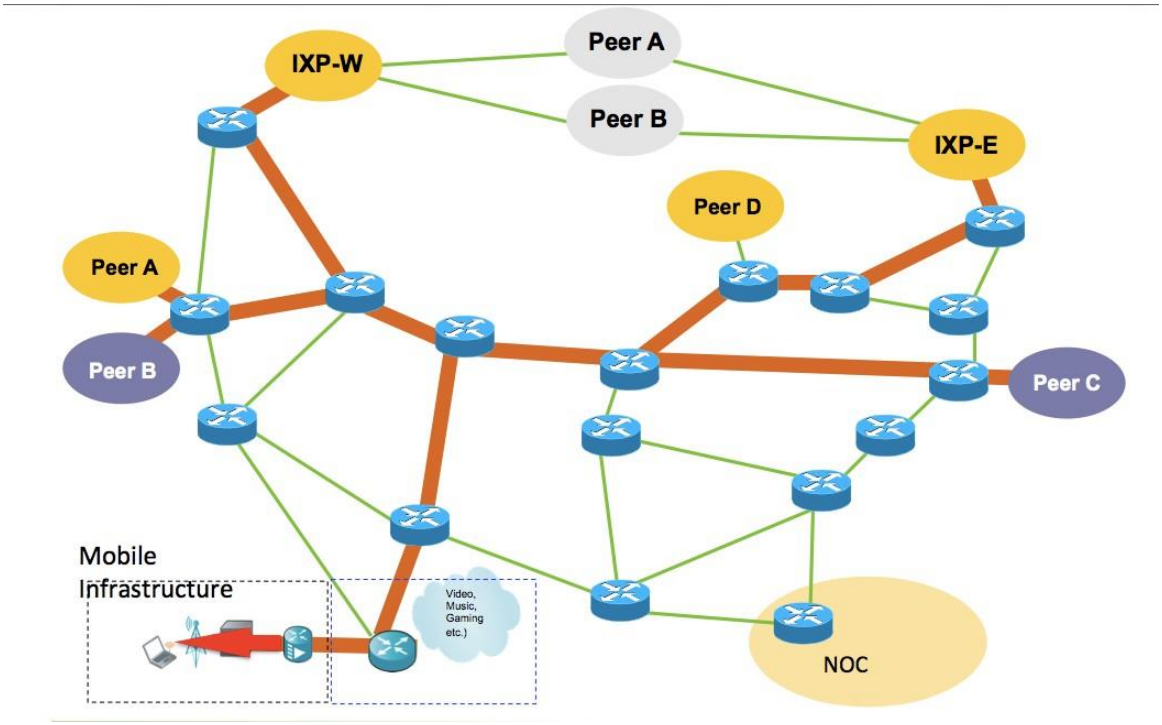
服务器/服务/应用程序不可用，拓扑接近目标网络的旁观者的互联网访问。

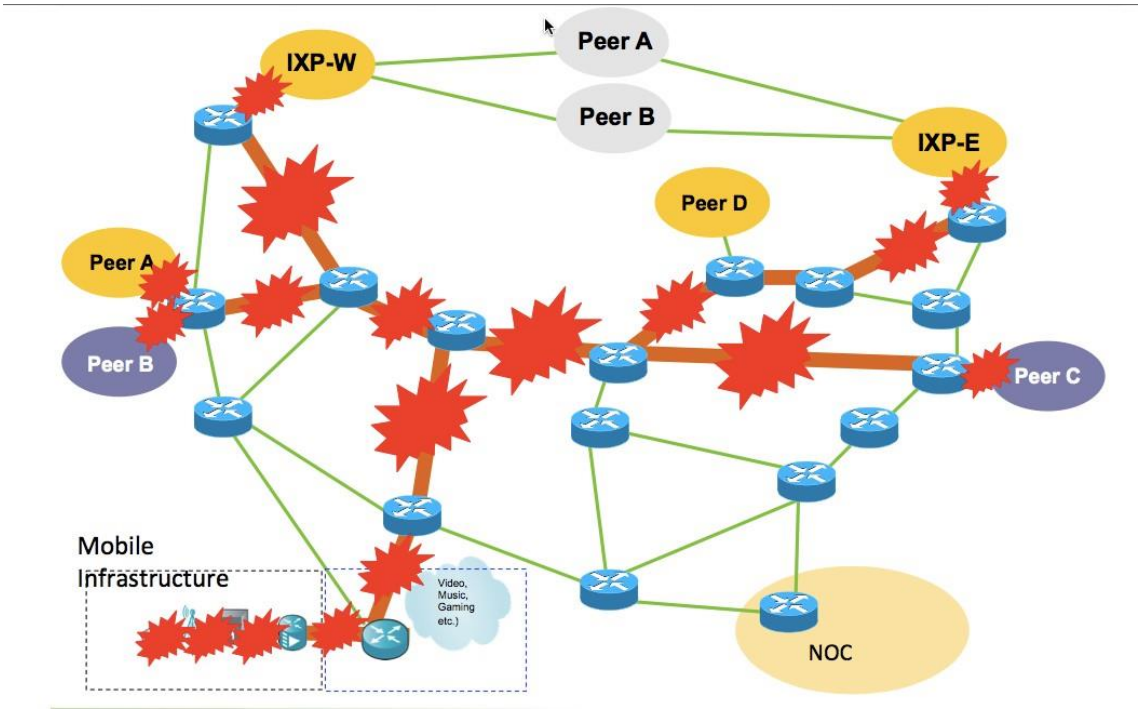

Authoritative
DNS Servers for
example.com
Abusable
Recursive
DNS
Servers
Internet-Accessible Servers, Routers, Home CPE devices, etc.
Compromised server
Attack source
IP-Address/32


Authoritative
DNS Servers for
example.com
Abusable
Recursive
DNS
Servers
UDP/1988 – UDP/53, ~70 bytes
Spoofed Source: 172.19.234.6
Destinations: Multiple Authoritative DNS servers
DNS query: TXT PGP.EXAMPLE.COM
Compromised server
Attack source
IP-Address/32


Impact
Impact
Authoritative DNS Servers for example.com
Impact
Impact
Impact
Impact
Abusable Recursive DNS Servers
UDP/53 – UDP/1988, ~8192 bytes, fragmented
Non-Spoofed Sources: Multiple Recursive DNS Servers
Destination: 172.19.234.6
DNS Response: TXT RR for PGP.EXAMPLE.COM
Compromised server
Attack source
Impact
IP-Address/32


IXP-W
Peer A
Peer B
IXP-E
Peer D
Peer A
Peer B
Peer C
Mobile Infrastructure
Video, Music, Gaming etc.)
NOC


IXP-W
Peer A
Peer B
IXP-E
Peer D
Peer A
Peer B
Peer C
Mobile
Infrastructure
Video,
Music,
Gaming
etc.)
NOC


IXP-W
Peer A
Peer B
IXP-E
Peer D
Peer A
Peer B
Peer C
Mobile
Infrastructure
Video,
Music,
Gaming
etc.)
NOC

附录E：最佳实践

最佳实践简介

最佳实践是指描述行业针对自身解决问题的最佳方法的指南。它们来自无与伦比的行业合作，需要大量专业知识和大量资源。最佳实践的主要目标是为组装行业的专业知识和经验提供指导。最佳实践的实施是自愿的。打算由负责任的组织（例如，服务提供商，网络运营商或设备供应商）决定是否实施特定的最佳做法。此外，每种最佳实践在特定情况下的适用性还取决于许多因素，这些最佳实践经验丰富的专家必须在同一领域内针对同一领域解决这一问题。

CSRIC IV工作组5推荐的最佳实践旨在提供指导。打算由负责任的组织（例如，服务提供商，网络运营商或设备供应商）决定是否实施特定的最佳做法。强制实施这些最佳实践与其意图不一致。这些最佳实践的适当应用只能由对公司特定网络基础架构架构有足够了解的个人理解其含义。尽管最佳实践的编写易于理解，但对于缺乏这种先决知识和经验的人来说，其含义通常并不明显。适当的应用程序需要了解最佳实践对系统，流程，组织，网络，订户，业务运营，复杂的成本问题和其他考虑因素的影响。考虑到有关预期用途的这些重要考虑因素，行业利益相关者担心，政府当局可能会不当地将其强加为法规或法院命令。由于这些最佳实践是根据广泛的行业合作开发而成的，需要广泛的专业知识和大量自愿资源，因此，如果滥用这些最佳实践，可能会损害行业将来共同提供此类指导的意愿。[29]

29这些原则来自NRIC VII焦点小组3B的工作，公共数据网络可靠性最终报告，第2.3.2和3.4.2节。

WG5确定了以下类别的最佳实践，以减轻基于服务器的分布式拒绝服务攻击：

备作
认证
分类
追溯
反应
事后形态与恢复
以下最佳实践解决了基于服务器的分布式拒绝服务攻击。

网络运营商

准备工作

BP编号：新的BP2
基于目的地的黑洞过滤/远程触发基于目的地的黑洞过滤：
网络运营商应部署基于目的地的黑洞过滤（BHF），以保护其网络免受分布式拒绝服务攻击。网络运营商应在可行的情况下为客户的IP空间提供客户发起的远程触发目的地黑洞过滤（RTBHF）。
BP参考/评论：
RFC 4778可用作初始响应，用于控制攻击，同时验证攻击影响和重新配置网络。
请注意，一旦实施黑洞过滤，它将通过丢弃所有流向目的地的流量来完成分布式拒绝服务攻击。可以通过向目标分配新的IP地址并发布新的DNS记录，恢复到目标的流量。 阶段：准备（部署缓解工具，网络运营商，托管过滤）
实施指南：有效性（H / M / L）：H
实施难度：（H / M / L）：M

BP编号：新的BP8
部署反欺骗技术：
网络运营商和主机提供商应在可行的情况下部署反欺骗技术，防止欺骗流量源自其网络。
BP参考/评论：
关于BP 9-7-0408
请注意，由于需要非对称路由，因此在某些多宿主网络上部署可能不可行。
阶段：准备（保护，网络运营商，托管服务提供商）

实施指南：有效性（H / M / L）：单个
家庭网络：H
多宿主网络：M到L
实施难度：（H / M / L）：
单家庭网络：L
多家庭网络：H

BP编号：新的BP16
部署网络数据清理：
网络运营商应在可行的情况下，使用网络数据清理中心过滤分布式拒绝服务攻击流量。这可以通过将可疑攻击分布式拒绝服务流量“隔离”到网络清理中心，在网络过滤中心过滤攻击流量，再将合法流量“重新隔离”回目标。

BP参考/评论：
重要的是，调整网络和清理中心的容量以容纳攻击流量，以便最大程度地减少流量激增引起的潜在附带损害。阶段：准备（部署缓解工具，网络运营商）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：H

血压编号：9-8-8047
防范DNS（域名系统）拒绝服务攻击：
网络运营商应通过提供深度防御，通过实施以下保护技术来防止可能使域名系统不可用的攻击，从而提供域名系统拒绝服务保护：

1) 通过冗余和强大的网络连接提高域名系统的弹性，例如，为每项服务部署具有不同网络连接的多台服务器，使任何一台服务器或站点均不影响其他服务器或站点。部署任播以提高其域名系统服务器的冗余性。任播可以用于利用网络中的多个域名服务器从单个域名服务器地址提供域名服务，从而提高域名系统的弹性。请注意，任播地址网络冗余，不提供域名系统（DNS）节点之间的负载平衡。
2) 具有用于内部和外部流量的独立名称服务器以及关键基础设施（如OAM&P和信令/控制网络），
3) 在可行的情况下，将缓存或递归域名系统与授权域名系统分开，
4) 通过使用适当配置的防火墙/过滤规则保护主域名服务器，实现所有名称解析的辅助主域名，并使用访问控制列表将区域传输请求限制到授权方，保护域名服务器信息。
5) 配置网络工具，以警告提供商的运营团队异常流量。
6) 将域名系统（DNS）网络过滤设计为域名系统（DNS）体系结构，以便在攻击期间对特定域名系统流量（域，查询类型，源IP，查询速率等）进行网络和应用级过滤；必须预先配置。此配置应将对合法域名系统流量的干扰降至最低。
7) 具有域名系统（DNS）服务器的带外管理连接，因此可以在攻击期间进行管理。
8) 将缓存DNS服务器与权威服务器分开。
9) 请勿将面向互联网的域名系统（DNS）服务器用于内部网络运营，管理，维护和供应系统。
10) 提供强大的域名系统（DNS）服务器和带宽容量，超过最大网络连接流量

BP参考/评论：
RFC-2870，ISO / IEC 15408，ISO 17799，US-CERT“保护互联网名称服务器”（）。
http://www.cert.org/archive/pdf/dns.pdf
阶段：准备（容量和资源，网络运营商）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：H

BP号：9-8-8753A –新BP（以前的BP 9-8-8563）
更新为：
漏洞管理-通知：
当发现拒绝服务或分布式拒绝服务漏洞或利用时，网络运营商，主机提供商和硬件/软件供应商应将此问题通知受影响的系统的所有者/运营商，确保更新软件，配置或设备以补救漏洞。如果不可能进行短期补救，则所有者/运营商应考虑采用系统或网络缓解措施，以最大程度地利用分布式拒绝服务攻击。
BP参考/评论：
Sans研究所，“漏洞管理：工具，挑战和最佳实践”。 2003。 12-13
准备（保护）BP
阶段：准备（保护，网络运营商，托管服务提供商）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：H

BP编号：9-9-8068
服务提供商，网络运营商，主机提供商，公共安全和设备供应商应制定和实施通信计划，作为更广泛的事件响应计划的一部分，确定关键参与者并酌情包括以下多个项目：联系人姓名，公司电话号码，家庭电话号码，寻呼机号码，传真号码，手机号码，家庭地址，互联网地址，永久网桥号码等。应在必要时在事件/事件发生之前制定通知计划。该计划还应包括备用通信渠道（例如，阿尔法传呼机，互联网，卫星电话，VOIP，专用线路，智能电话），平衡任何备用方法的价值与引入的安全和信息丢失风险。
BP参考/评论：
备用宽带通信路径，用于协调和管理。阶段：准备（通信，网络运营商，
托管提供商）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：L

血压编号：9-8-8753
更新为：
漏洞管理：
网络运营商，主机提供商和硬件/软件供应商应确保可以管理为客户管理或维护的产品中的安全漏洞。这样的管理可以是被动的，例如仅维护已向其分发产品的客户列表，也可以是主动的（例如漏洞扫描和报告）。此外，应在大规模部署之前测试产品，服务，硬件和软件的漏洞。

BP参考/评论：
Sans研究所，“漏洞管理：工具，挑战和最佳实践”。 2003。 12-13
准备（保护）BP
阶段：准备（保护，网络运营商，托管服务提供商）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：H

血压编号：9-8-8912
与其他网络运营商沟通态势感知和保护措施的实施：
网络运营商应通过手动或自动方法发送和/或接收滥用报告，做出合理的努力与其他运营商和安全软件提供商进行通信。对于分布式拒绝服务攻击而言，将其参与攻击通知分布式拒绝服务流量源尤为重要。需要这种信息共享和协作来帮助防止将来的攻击。这些努力可以包括诸如实施“保护措施”之类的信息，诸如使用诸如滥用报告格式（ARF）之类的标准消息格式经由反馈环（FBL）报告滥用（例如，垃圾邮件）。在可行的情况下，网络运营商应与其他行业参与者和互联网生态系统的其他成员共同努力，以期在私营部门提供商之间的僵尸网络检测领域实施更强大，标准化的信息共享。
BP参考/评论：
请注意，与其他网络运营商的通信机制应在攻击发生之前进行，以便在攻击期间如有必要，提供通信通道。
有关更多信息，请参见以下文档：
http://www.maawg.org/sites/maawg/files/news/CodeofConduct.pdf
可以使用以下位置提供的信息以标准方式报告漏洞：http://nvd.nist.gov/
http://puck.nether.net/mailman/listinfo/nsp-security
https://ops-trust.net/
https://stix.mitre.org/https://www2.icsalabs.com/veris/
阶段：准备（通信，网络运营商）后期制作和恢复
实施指导：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：M

请注意，该类别中的最佳实践主要针对向住宅宽带网络上的消费者最终用户提供服务的互联网服务提供商，但也可能适用于其他用户和网络。

血压编号：9-8-8917
通知最终用户：
网络运营商和主机提供商应开发和维护关键的通知方法，与客户沟通其计算机，服务器和/或网络可能感染了恶意软件。其中应包括一系列选项，以适应不同类型的客户和网络技术。一旦网络运营商检测到可能的最终用户安全问题，应立即采取措施通知互联网用户他们可能存在安全问题。网络运营商或主机托管提供商应决定向其客户或互联网用户提供通知的最适当方法，如果所选方法无效，则应使用其他方法。通知选项的范围可能会因问题的严重性和/或严重性而异。
不同的通知方法的示例可以包括但不限于：电子邮件，电话，邮政邮件，即时消息（IM），短信服务（SMS）和网络浏览器通知。
BP参考/评论：
网络运营商和主机托管提供商决定采用最合适的方法向一个或多个客户或互联网用户发送通知的决定取决于一系列因素，从网络运营商的技术能力到网络的技术属性运营商网络，成本考虑因素，可用服务器资源，可用组织资源，在任何给定时间检测到的可能感染主机的数量以及任何可能威胁的严重性等许多其他因素。对于网络运营商来说，使用多种同时通知方法是合理的，但对于虚构的反病毒提供商而言可能很难。请注意，发现盲通知（即不跟进通知）的使用效果不如验证或要求用户采取措施的方法有效。最佳实践9-8-8921提供了有关如何解决恶意软件感染的信息。https://otalliance.org/best-practices/industry-best-practices
有关更多信息，请参见：
https://otalliance.org/system/files/files/resource/documents/ota_botnet_notification_whitepaper2012.pdf
阶段：准备（通信，网络运营商，托管提供商）
实施指南：　　有效性（H / M / L）：L
　　实施难度：（H / M / L）：M

请注意，该类别中的最佳实践主要针对向住宅宽带网络上的消费者最终用户提供服务的互联网服务提供商，但也可能适用于其他用户和网络。

血压编号：8-9-8074
更新时间
拒绝服务（DoS）攻击-目标：
在可行的情况下，网络运营商，主机提供商和目标网络及设备供应商设备应能够承受数据包数量和带宽利用率大幅增长的影响。在可行的情况下，设备和软件供应商应为其产品系列开发有效的拒绝服务/分布式拒绝服务生存能力功能。

支持关键任务服务的基础设施应设计为显着增加流量，并且必须包括能够过滤和/或限制速率的流量的网络设备。网络工程师必须了解设备的功能以及如何最大程度地利用它们。无论何时何地，关键任务系统都应在集群配置中部署，以实现多余流量的负载平衡，并由专用的拒绝服务/分布式拒绝服务保护设备保护。关键基础设施运营商应尽可能部署可拒绝服务拒绝服务的硬件和软件。

BP参考/评论：

注意：此最佳做法可能会影响9-1-1的操作。

例如，SYN泛洪攻击防御，CERT /CC®咨询CA-1996-21 TCP SYN泛洪和IP欺骗攻击-与NRIC BP 8753A有关。http://www.cert.org/advisories/CA-1996-21.html.

请注意，网络运营商，主机提供商，目标和设备供应商需要确定哪些服务对于实施此最佳实践至关重要。

阶段：准备（容量和资源，网络运营商，托管提供商，目标）

实施指南：　　有效性（H / M / L）：M

　　实施难度：（H / M / L）：H

血压编号：9-9-8725

更新为：

信令拒绝服务保护：

网络运营商应为各种流量指标建立报警阈值，确保识别拒绝服务/拒绝服务条件。例如，将关键网络点正常流量水平的基准与当前流量水平进行比较，并将流量水平和协议的网络流信息的基线与当前流量水平进行比较。

BP参考/评论：

注意：此最佳做法可能会影响9-1-1的操作。

警报阈值旨在识别可能对运营商基础设施构成威胁的拒绝服务条件。

阶段：准备（监控和可见性，网络运营商）

实施指南：　　有效性（H / M / L）：H

　　实施难度：（H / M / L）：M

BP号：新的BP3污水坑

路由：

网络运营商应部署Sinkhole路由，将攻击流量路由到网络的其他部分进行分析（Sinkholing）和丢弃（Offramping）。

BP参考/评论：

阶段：准备（部署缓解工具，网络运营商，托管过滤）

实施指南：　　有效性（H / M / L）：M

　　实现难度：（H / M / L）：H

RFC 4778可与任播一起使用以提供冗余。

BP编号：新的BP4
基于信号源的黑洞滤波：
网络运营商应部署基于源黑洞过滤（SBBHF）或类似的动态机制，根据源数据包标头信息触发网络范围的过滤，以保护其网络免受分布式拒绝服务攻击。请注意，如果在攻击中使用大量或源IP地址（例如僵尸网络攻击），或者攻击流量使用欺骗性IP地址进行混淆，此方法可能无效。
BP参考/评论：
格林，巴里·拉文丹德兰（Barry Raveendran）。“**第一**阶段-**使用IP路由作**为安全工具，准备工具和技术。” ISP Security Bootcamp Singapore2003。2003**年7月31日**ftp://ftp-eng.cisco.com/cons/isp/security/ISP-Security-Bootcamp-Singapore-2003/H-Preparation-Tools-v3-0.pdf
阶段：准备（部署缓解工具，网络运营商，托管过滤）
实施指南：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：M

BP编号：新的BP5
部署流量过滤器自动分发：
网络运营商应部署BGP Flowspec等系统，在发生DOS / DDoS攻击时自动将流量过滤器分配到相关设备，这些系统可以过滤到目标的攻击流量，同时允许合法流量通过。

BP参考/评论：
RFC 5575，RFC 4360
阶段：准备（部署缓解工具，网络运营商，托管过滤）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：H
请注意，当前并非所有路由器供应商都支持该技术。

BP编号：新的BP9
区分流量优先级以确保关键流量（例如控制平面）不受基于服务器的DDOS攻击的影响：
网络运营商应将控制平面和其他关键流量的优先级高于转接流量，以确保分布式拒绝服务攻击流量不会影响路由协议的运行。
BP参考/评论：

阶段：准备（容量和资源，网络运营商）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：M

BP编号：新的BP14
防止DNS服务用于反射攻击：网络运营商应采取保护措施，防止其域名系统服务被入侵

如果可行，用作反射攻击的一部分。这些保护可能包括但不限于：

1. 限制递归域名系统（DNS）服务器仅响应来自服务所需的最小实际 IP 子网集合的查询。
2. 实施检测和警报流程，以检测攻击中滥用的域，IP 和服务器。
3. 配置控件以允许缓解特定攻击，如查询速率限制，移除特定域或过滤检测到攻击时可以应用的查询类型。
4. 具有流量异常检测和响应能力。
5. 酌情部署域名系统协议验证系统，以丢弃非法或恶意域名系统流量。

BP参考/评论：
该BP代替BP 9-8-8118
请注意，由于网络运营商控制的域名系统服务器数量比部署的域名系统服务器总数低，因此仅由网络运营商实施此最佳实践对使用开放式域名系统（DNS）服务器的总体问题产生的影响攻击率低。

阶段：准备（保护，网络运营商，容量和资源，网络运营商）
实施指导：　　有效性（H / M / L）：L
　　实施难度：（H / M / L）：M

鉴定

BP号码：9-8-8916
更新为：
僵尸检测和相应的通知应及时：
网络运营商和托管提供商应确保及时进行僵尸程序检测以及向托管客户的相应通知，因为此类安全问题对时间敏感。如果需要复杂的分析并且需要多次确认以确认确实存在机器人，那么恶意软件可能会对被感染的主机或远程定位系统造成一定程度的损害（超出初始感染的损害）。可以停止。因此，网络运营商或托管提供商必须在确定确认恶意软件感染（可能需要花费较长时间）的需求与预测非常短时间内恶意软件感染可能性很大的能力之间取得平衡。这项“最终vs.可能”挑战非常艰巨，如有疑问，网络运营商和主机提供商应谨慎行事，传达恶意软件感染信息，同时采取合理措施避免误报。
BP参考/评论：
网络运营商通知实施需要在检测到感染的确定性与短暂检测到恶意流量的不确定性之间取得平衡，以最大程度地降低假阳性通知的可能性，这种假阳性通知可能会使客户烦恼并变得难以管理。

有关更多信息，请参见美国互联网服务提供商反机器人行为守则（ABC）：
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

阶段：标识（监控和可见性，网络运营商，托管提供商）
实施指南：　　有效性（H / M / L）：L（仅通知）
　　实施难度：（H / M / L）：M

请注意，该类别中的最佳实践主要针对向住宅宽带网络上的消费者最终用户提供服务的互联网服务提供商，但也可能适用于其他用户和网络。

BP编号：新BP6
使用Netflow数据分析来分析分布式拒绝服务攻击：
在可行的情况下，网络运营商和主机提供商应启用，收集和分析Netflow**数据**，**以帮助**识别和分类分布式拒绝服务攻击。攻击后数据应该可用，以便进行进一步分析。
Netflow**数据的保留**应符合网络运营商的数据保留政策。
BP参考/评论：
Netflow数据可能有助于识别欺骗攻击。
阶段：标识（监控和可见性，网络运营商，托管服务提供商）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：M

血压编号：9-8-8913
维护检测机器人/恶意软件感染的方法：
网络运营商应维持检测客户设备可能恶意软件感染的方法。检测方法会因多种因素而有很大差异。检测方法，工具和流程可能包括但不限于：外部反馈，对网络状况和流量的观察（如带宽和/或流量模式分析），签名，行为技术以及更详细级别的客户取证监控。
BP参考/评论：
有关更多信息，请参见：
http://teamcymru.org
http://shadowserver.orgh
ttp://abuse.chhttp://cbl.a
buseat.org
美国互联网服务提供商反机器人行为守则（ABC）：
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

请注意，该类别中的最佳实践主要针对向住宅宽带网络上的消费者最终用户提供服务的互联网服务提供商，但也可能适用于其他用户和网络。
阶段：识别（监控和可见性，网络运营商）
实施指南：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：H

BP号码：9-8-8914
使用分层僵尸攻击检测方法：
网络运营商应使用分层方法进行僵尸网络检测，首先应用用户流量的行为特征（投射到广域网），然后对被标记为潜在问题的流量应用更精细的技术（例如签名检测）。
BP参考/评论：
除非有理由相信客户已感染，否则不收集详细信息，此技术应有助于最大程度地减少检测机器人程序时客户信息的暴露。
使用宽网络方法查看用户流量可以包括外部反馈以及其他内部方法。
为了限制对更复杂工具（如深度数据包检查和签名）的需求，此方法很有用。一旦怀疑恶意机器人流量（宽带网络），就可以对流量进行更详细的分析。
有关更多信息，请参见美国互联网服务提供商反机器人行为守则（ABC）：
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

阶段：识别（监控和可见性，网络运营商）
实施指南：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：H

请注意，该类别中的最佳实践主要针对向住宅宽带网络上的消费者最终用户提供服务的互联网服务提供商，但也可能适用于其他用户和网络。

分类

BP号：新的BP 18对DoS / DDoS攻击进行分类：
网络运营商，主机提供商和分布式拒绝服务目标（如果可行）应具有分析和分类拒绝服务/分布式拒绝服务攻击的流程和/或能力。攻击分类可以帮助确定最佳的攻击缓解措施，并帮助确定提供未来保护所需的改进。
BP参考/评论：
示例分类：容量攻击？
直接数据包洪水反射/放大应用层攻击？
状态或资源耗尽攻击？控制平面攻击？
Ipv6 特定攻击？

日期？阶段：分类（攻击类型，网络运营商，托管提供商，目标），事后技术与恢复（网络运营商，托管提供商，目标）
实施指南：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：H

追溯

BP号：9-8-0507：攻击溯源：
网络运营商应具有流程和/或能力，用于分析和确定恶意流量的来源，然后在源处或更靠近源的位置追溯和丢弃数据包。参考文献提供了几种不同的可能技术。（恶意流量是指设计和传输诸如分布式拒绝服务（DDoS）攻击，Smurf 和 Fraggle 攻击之类的流量，目的是消耗目标网络的资源来阻止服务，或者消耗资源到可能导致系统崩溃的状态）。
BP参考/评论：
华盛顿大学计算机科学与工程系，Stefan Savage 等人，“ IP 追溯的实用网络支持”，技术报告 UW-CSE-2000-02-01，版本发表于 2000 年会议论文集 ACM SIBCOMM pp256-306，瑞典斯德哥尔摩，2000 年 8 月。阶段：追溯（网络运营商）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：H

反馈

BP号码：9-9-8065
网络运营商和主机提供商应建立向执法人员发布信息的流程，并确定协调活动的联络点（POC）。
BP参考/评论：
没有阶段：反应（网络运营商，托管服务提供商）
实施指南：　　有效性（H / M / L）：L
　　实施难度：（H / M / L）：L

事后形态与恢复

BP号码：9-9-8762
从拒绝服务攻击中恢复：
更新为：
网络运营商和主机提供商应在可行的情况下，在发生重大网络事件期间和之后与其他组织合作，共享有关表征攻击特征的步骤，识别，过滤和隔离攻击源点的技术以及所采取措施的信息。重新路由合法流量并阻止或防御类似的拒绝服务攻击。
BP参考/评论：
IETF RFC2350，CMU / SEI-98-HB-001。注意：此最佳做法可能会影响9-1-1的操作。
更新后添加：
此最佳实践旨在从拒绝服务攻击中恢复运营商的基础设施。阶段：反应（网络运营商，托管服务提供商）；Post Mortem（网络运营商，托管服务提供商）
实施指导：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：M

血压编号：9-8-8515
更新为：
从滥用或不当使用系统资源中进行恢复：
如果检测到滥用行为或未经授权使用受其控制的系统（例如，检测到参与分布式拒绝服务攻击），则网络运营商，主机提供商或目标应在可行的情况下对系统进行取证分析，验尸分析，应用控制措施防止未来攻击和/或实施系统资源配额。 BP参考/评论：
IETF RFC2350，CMU / SEI-98-HB-001。
阶段：后期服务（网络运营商，托管提供商，目标）
实施指南：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：H

托管服务提供商

准备工作

BP编号：新的BP10
定期使用供应商提供的安全更新或新版本更新技术：
托管服务提供商应采取合理措施为客户提供最新的软件和插件（如果托管服务提供商提供软件）。供应商应积极支持向客户提供的软件以修复安全问题。
应向客户提供补丁工具，流程或说明，以帮助客户通过安全补丁使软件保持最新。在可行的情况下，选择提供自动安全更新并为客户提供有关如何激活更新的说明的软件。
BP参考/评论：
待定
阶段：准备（保护，托管服务提供商）

实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：H

BP号：9-8-8753（网络运营商部分重复）
更新为：
漏洞管理：
网络运营商，主机提供商和硬件/软件供应商应确保可以管理为客户管理或维护的产品中的安全漏洞。这样的管理可以是被动的，例如仅维护已向其分发产品的客户列表，也可以是主动的（例如漏洞扫描和报告）。此外，应在大规模部署之前测试产品，服务，硬件和软件的漏洞。
BP参考/评论：
Sans研究所，“漏洞管理：工具，挑战和最佳实践”。 2003。 12-13
准备（保护）BP
阶段：准备（保护，网络运营商，托管服务提供商）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：H
BP编号：9-8-8753A –新BP（以前的BP 9-8-8563）（从网络运营商部门重复）
更新为：
漏洞管理-通知：
当发现拒绝服务或分布式拒绝服务漏洞或利用时，网络运营商，主机提供商和硬件/软件供应商应将此问题通知受影响的系统的所有者/运营商，以确保将软件，配置或设备更新为

补救漏洞。如果不可能进行短期补救，则所有者/运营商应考虑采用系统或网络缓解措施，以最大程度地利用分布式拒绝服务攻击。

BP参考/评论：

Sans研究所，“漏洞管理：工具，挑战和最佳实践”。 2003。 12-13

准备（保护）BP

阶段：准备（保护，网络运营商，托管服务提供商）

实施指南：　　有效性（H / M / L）：H

　　实施难度：（H / M / L）：H

BP号：9-8-8917（网络运营商部分重复）通知最终用户：

网络运营商和主机提供商应开发和维护关键的通知方法，与客户沟通其计算机，服务器和/或网络可能感染了恶意软件。其中应包括一系列选项，以适应不同类型的客户和网络技术。一旦网络运营商检测到可能的最终用户安全问题，应立即采取措施通知互联网用户他们可能存在安全问题。网络运营商或主机托管提供商应决定向其客户或互联网用户提供通知的最适当方法，如果所选方法无效，则应使用其他方法。通知选项的范围可能会因问题的严重性和/或严重性而异。

不同的通知方法的示例可以包括但不限于：电子邮件，电话，邮政邮件，即时消息（IM），短信服务（SMS）和网络浏览器通知。

BP参考/评论：

网络运营商和主机托管提供商决定采用最合适的方法向一个或多个客户或互联网用户发送通知的决定取决于一系列因素，从网络运营商的技术能力到网络的技术属性运营商网络，成本考虑因素，可用服务器资源，可用组织资源，在任何给定时间检测到的可能感染主机的数量以及任何可能威胁的严重性等许多其他因素。对于网络运营商来说，使用多种同时通知方法是合理的，但对于虚构的反病毒提供商而言可能很难。请注意，发现盲通知（即不跟进通知）的使用效果不如验证或要求用户采取措施的方法有效。最佳实践9-8-8921提供了有关如何解决恶意软件感染的信息。https://otalliance.org/best-practices/industry-best-practices

有关更多信息，请参见：

https://otalliance.org/system/files/files/resource/documents/ota_botnet_notification_whitepaper2012.pdf

阶段：准备（通信，网络运营商，托管提供商）

实施指南：　　有效性（H / M / L）：L

　　实施难度：（H / M / L）：M

请注意，该类别中的最佳实践主要针对向住宅宽带网络上的消费者最终用户提供服务的互联网服务提供商，但也可能适用于其他用户和网络。

BP号码：9-8-8901
更新为：
托管服务提供商对计算机卫生/安全计算教育资源的支持：
托管服务提供商应向客户提供，提供，识别或支持第三方教程，教育和自助资源，以教育客户重要性以及帮助他们实践安全计算。托管服务提供商客户应了解如何通过各种方法保护终端用户设备和网络免遭未经授权的访问，包括但不限于：

1) 使用合法的安全软件防御病毒和间谍软件；
2) 确保任何软件下载或购买均来自合法来源；
3) 使用防火墙；
4) 维护操作系统，数据库，应用程序和应用程序插件的最新安全补丁；
5) 向客户宣传漏洞管理和扫描的重要性。
6) 删除并停止使用未安装安全补丁的软件；
7) 定期扫描服务器上的恶意软件，间谍软件和其他潜在有害软件；
8) 保持所有应用程序，应用程序插件和操作系统软件为最新和更新，并使用其安全功能；
9) 使用强密码和/或二元身份验证；10）禁止共享密码。
11）提供联系信息以报告问题。

BP参考/评论：
有关更多信息，请参见：
国家网络安全联盟-http://www.staysafeonline.org/
OnGuard在线-http://www.onguardonline.gov/default.aspx
国土安全部-
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
阶段：准备（教育，托管服务提供商）
实施指南：　　有效性（H / M / L）：L
　　实施难度：（H / M / L）：L

请注意，该类别中的最佳实践主要针对向住宅宽带网络上的消费者最终用户提供服务的互联网服务提供商，但也可能适用于其他用户和网络。

BP号：9-9-8068（网络运营商部分重复）
服务提供商，网络运营商，主机提供商，公共安全和设备供应商应制定和实施通信计划，作为更广泛的事件响应计划的一部分，确定关键参与者并酌情包括以下多个项目：联系人姓名，公司电话号码，家庭电话号码，寻呼机号码，传真号码，手机号码，家庭地址，互联网地址，永久网桥号码等。应在必要时在事件/事件发生之前制定通知计划。该计划还应包括备用通信渠道（例如，阿尔法传呼机，互联网，卫星电话，VOIP，专用线路，智能电话），平衡任何备用方法的价值与引入的安全和信息丢失风险。
BP参考/评论：
备用宽带通信路径，用于协调和管理。阶段：准备（通信，网络运营商，
托管提供商）　　实施指南：有效性（H / M / L）：H
实施难度：（H / M / L）：L

BP码：8-9-8074（网络运营商部分重复）已更新
拒绝服务（DoS）攻击-目标：（从网络运营商部分重复）在可行的情况下，网络运营商，主机提供商，目标网络和设备供应商设备应能够应对数据包数量和带宽利用率大幅增长的情况。在可行的情况下，设备和软件供应商应为其产品系列开发有效的拒绝服务/分布式拒绝服务生存能力功能。
支持关键任务服务的基础设施应设计为显着增加流量，并且必须包括能够过滤和/或限制速率的流量的网络设备。网络工程师必须了解设备的功能以及如何最大程度地利用它们。无论何时何地，关键任务系统都应在集群配置中部署，以实现多余流量的负载平衡，并由专用的拒绝服务/分布式拒绝服务保护设备保护。关键基础设施运营商应尽可能部署可拒绝服务拒绝服务的硬件和软件。
BP参考/评论：
注意：此最佳做法可能会影响9-1-1的操作。

例如，SYN泛洪攻击防御，CERT /CC®咨询CA-1996-21 TCP SYN泛洪和IP欺骗攻击-与NRIC BP 8753A有关。http://www.cert.org/advisories/CA-1996-21.html.
请注意，网络运营商，主机提供商，目标和设备供应商需要确定哪些服务对于实施此最佳实践至关重要。
阶段：准备（容量和资源，网络运营商，托管提供商，目标）
实施指南：　　有效性（H / M / L）：M
实施难度：（H / M / L）：H

BP号码：新BP8（网络运营商部分重复）部署反欺骗技术：
网络运营商和主机提供商应在可行的情况下部署反欺骗技术，防止欺骗流量源自其网络。
BP参考/评论：
关于BP 9-7-0408
请注意，由于需要非对称路由，因此在某些多宿主网络上部署可能不可行。
阶段：准备（保护，网络运营商，托管服务提供商）

实施指南：　　有效性（H / M / L）：H
实施难度：（H / M / L）：
单家庭网络：L
多家庭网络：H

BP编号：新的BP1
基于应用的网络保护：
托管服务提供商和攻击来源应考虑利用基于应用程序的网络和/或基于主机的入侵检测系统，防火墙或其他安全设备（默认配置为拒绝流量），以防范托管中心中恶意或未经授权的传入或传出网络流量或在服务器上。 BP参考/评论：
GB973指南-4 / DSD 2011＃8（修改版）
GB973指南-5 / DSD 2011＃9（修改版）
例如：利用边界控制功能（例如会话边界控制器或类似设备），通过阻止来自服务器场（未经授权的端点）的注册风暴并阻止协议模糊测试，防止VOIP通信拒绝/降级。
请注意，确保部署的应用程序保护自身不容易遭受拒绝服务/分布式拒绝服务攻击非常重要。如果其设计或配置使其很容易受到设备攻击，则可能会使应用程序更容易受到分布式拒绝服务攻击。
阶段：准备（预防，托管服务提供商）
实施指南：　　有效性（H / M / L）：M
实施难度：（H / M / L）：M

鉴定

BP编号：针对恶意或分布式拒绝服务流量托管环境的新BP11监控：
托管服务提供商应在可行的情况下监控其环境中是否存在恶意或分布式拒绝服务网络流量，以识别攻击源和攻击方法。
BP参考/评论：
TBD 阶段：识别（托管服务提供商）
实施指南：　　有效性（H / M / L）：H
实施难度：（H / M / L）：M

BP号：9-8-8916（网络运营商部分重复）
更新为：
僵尸检测和相应的通知应及时：
网络运营商和托管提供商应确保及时进行僵尸程序检测以及向托管客户的相应通知，因为此类安全问题对时间敏感。如果需要复杂的分析并且需要多次确认以确认确实存在机器人，那么恶意软件可能会对被感染的主机或远程定位系统造成一定程度的损害（超出初始感染的损害）。可以停止。因此，网络运营商或托管提供商必须在确定确认恶意软件感染（可能需要花费较长时间）的需求与预测非常短时间内恶意软件感染可能性很大的能力之间取得平衡。这项"最终vs.可能"挑战非常艰巨，如有疑问，网络运营商和主机提供商应谨慎行事，传达恶意软件感染信息，同时采取合理措施避免误报。
BP参考/评论：
网络运营商通知实施需要在检测到感染的确定性与短暂检测到恶意流量的不确定性之间取得平衡，以最大程度地降低假阳性通知的可能性，这种假阳性通知可能会使客户烦恼并变得难以管理。
有关更多信息，请参见美国互联网服务提供商反机器人行为守则（ABC）：
http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf

阶段：标识（监控和可见性，网络运营商，托管提供商）
实施指南：　　有效性（H / M / L）：L（仅通知）
　　实施难度：（H / M / L）：M

请注意，该类别中的最佳实践主要针对向住宅宽带网络上的消费者最终用户提供服务的互联网服务提供商，但也可能适用于其他用户和网络。

BP号码：新BP6（网络运营商部分重复）使用Netflow数据分析分析
分布式拒绝服务攻击：
在可行的情况下，网络运营商和主机提供商应启用，收集和分析Netflow**数据**，**以帮助**识别和分类分布式拒绝服务攻击。攻击后数据应该可用，以便进行进一步分析。
Netflow**数据的保留**应符合网络运营商的数据保留政策。
BP参考/评论：
Netflow数据可能有助于识别欺骗攻击。
阶段：标识（监控和可见性，网络运营商，托管服务提供商）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：M

分类

BP号码：新的BP18（从网络运营商部分重复）分类拒绝服务/分布式拒绝服务攻击：

网络运营商，主机提供商和分布式拒绝服务目标（如果可行）应具有分析和分类拒绝服务/分布式拒绝服务攻击的流程和/或能力。攻击分类可以帮助确定最佳的攻击缓解措施，并帮助确定提供未来保护所需的改进。

BP参考/评论：

示例分类：

容量攻击？

直接数据包洪水反射/放大

应用程序层攻击？

状态或资源耗尽攻击？控制平面攻击？

Ipv6特定攻击？日期？

阶段：分类（攻击类型，网络运营商，托管服务提供商，目标），后期技术和恢复（网络运营商，托管提供商，目标）

实施指导：　　有效性（H / M / L）：M

实施难度：（H / M / L）：H

追溯

反应

BP号：新的BP12通知托管客户恶意或分布式拒绝服务流量

托管服务提供商应在可行的情况下，如果检测到从其服务器发出恶意或分布式拒绝服务网络流量，则应通知受影响的客户，并在适当时协助客户进行补救。

BP参考/评论：

待定待定阶段：反应（托管服务提供商）

实施指南：　　有效性（H / M / L）：M

实施难度：（H / M / L）：H

BP号：9-9-8065（网络运营商部门重复）

网络运营商和主机提供商应建立向执法人员发布信息的流程，并确定协调活动的联络点（POC）。

BP参考/评论：
没有阶段：反应（网络运营商，托管服务提供商）
实施指南：　　有效性（H / M / L）：L
　　实施难度：（H / M / L）：L

事后形态与恢复

BP号：9-9-8762（网络运营商部分重复）从拒绝服务攻击中恢复：
更新为：
网络运营商和主机提供商应在可行的情况下，在发生重大网络事件期间和之后与其他组织合作，共享有关表征攻击特征的步骤，识别，过滤和隔离攻击源点的技术以及所采取措施的信息。重新路由合法流量并阻止或防御类似的拒绝服务攻击。
BP参考/评论：
IETF RFC2350，CMU / SEI-98-HB-001。注意：此最佳做法可能会影响9-1-1的操作。
更新后添加：
此最佳实践旨在从拒绝服务攻击中恢复运营商的基础设施。阶段：反应（网络运营商，托管服务提供商）；Post Mortem（网络运营商，托管服务提供商）
实施指导：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：M

BP号：（从网络运营商部门重复）9-8-8515
更新为：
从滥用或不当使用系统资源中进行恢复：
如果检测到滥用行为或未经授权使用受其控制的系统（例如，检测到参与分布式拒绝服务攻击），则网络运营商，主机提供商或目标应在可行的情况下对系统进行取证分析，验尸分析，应用控制措施防止未来攻击和/或实施系统资源配额。 BP参考/评论：
IETF RFC2350，CMU / SEI-98-HB-001。
阶段：后期服务（网络运营商，托管提供商，目标）
实施指南：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：H

目标

准备工作

BP码：8-9-8074（网络运营商部分重复）已更新
拒绝服务（DoS）攻击-目标：
在可行的情况下，网络运营商，主机提供商和目标网络及设备供应商设备应能够承受数据包数量和带宽利用率大幅增长的影响。在可行的情况下，设备和软件供应商应为其产品系列开发有效的拒绝服务/分布式拒绝服务生存能力功能。支持关键任务服务的基础设施应设计为显着增加流量，并且必须包括能够过滤和/或限制速率的流量的网络设备。网络工程师必须了解设备的功能以及如何最大程度地利用它们。无论何时何地，关键任务系统都应在集群配置中部署，以实现多余流量的负载平衡，并由专用的拒绝服务/分布式拒绝服务保护设备保护。关键基础设施运营商应尽可能部署可拒绝服务拒绝服务的硬件和软件。
BP参考/评论：
注意：此最佳做法可能会影响9-1-1的操作。

例如，SYN泛洪攻击防御，CERT /CC®咨询CA-1996-21 TCP SYN泛洪和IP欺骗攻击-与NRIC BP 8753A有关。http://www.cert.org/advisories/CA-1996-21.html.
请注意，网络运营商，主机提供商，目标和设备供应商需要确定哪些服务对于实施此最佳实践至关重要。
阶段：准备（容量和资源，网络运营商，托管提供商，目标）
实施指南：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：H

BP编号：新的BP7
网络服务应限制可能导致网络服务器出站带宽拥塞的有效负载：
网络应用程序提供商应限制大型对象（如大型文档下载），以防止重复请求占用服务器的大量出站带宽（即服务器站点到客户端站点的带宽），这可能会导致合法用户出现拒绝服务条件。另外，请考虑限制在特定时间范围内每个IP地址允许的HTTP Get / Post请求数量。
BP参考/评论：
待定
阶段：准备（最小化攻击面，目标）
实施指南：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：H

BP编号：新的BP13
监控目标恶意或分布式拒绝服务流量：
目标应监控安全和服务器日志，以确定是否发生了异常流量或安全事件。这有助于确定目标是否受到攻击或最近是否发生过攻击；它也可能表示攻击的先兆。
BP参考/评论：
请注意，攻击的目标可以是最终用户，网络运营商和主机提供商。
阶段：准备（监控和可见性，目标）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：M

BP编号：新的BP15
利用内容交付网络提供应用程序稳健性：
攻击目标应利用内容交付网络（CDN）提供鲁棒性，以最大程度地降低对拒绝服务/分布式拒绝服务攻击的敏感性。 CDN可以用于在整个网络上分配应用程序功能，使其更强大地抵御拒绝服务/分布式拒绝服务攻击。
BP参考/评论：
待定
阶段：准备（部署缓解工具，目标）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：L

BP编号：新的BP17
部署现场目标数据清理：
分布式拒绝服务目标可能会使用流量数据清理中心过滤分布式拒绝服务攻击流量。这可以通过将可疑攻击分布式拒绝服务流量“分流”到现场清理中心来过滤攻击流量，再将合法流量“爬坡”回目标。
BP参考/评论：
调整站点网络和清理中心的容量以容纳攻击流量非常重要，这样才能最大程度地减少流量激增造成的潜在附带损害。
阶段：准备（部署缓解工具，托管过滤）
实施指南：　　有效性（H / M / L）：H
　　实施难度：（H / M / L）：H

鉴定

分类

BP号码：新的BP18（从网络运营商部分重复）分类拒绝服务/分布式拒绝服务攻击：

网络运营商，主机提供商和分布式拒绝服务目标（如果可行）应具有分析和分类拒绝服务/分布式拒绝服务攻击的流程和/或能力。攻击分类可以帮助确定最佳的攻击缓解措施，并帮助确定提供未来保护所需的改进。

BP参考/评论：

示例分类：

容量攻击？

直接数据包洪水反射/放大

应用程序层攻击？

状态或资源耗尽攻击？控制平面攻击？

Ipv6特定攻击？日期？

阶段：分类（攻击类型，网络运营商，托管提供商，目标），事后与恢复（网络运营商，托管提供商，目标）

实施指导：

有效性（H / M / L）：M

实施难度：（H / M / L）：H

追溯反应

事后形态与恢复

BP码：9-8-8561从拒绝服务攻击中恢复-目标：

如果在目标控制下的网络元素，系统或服务器遭受了拒绝服务或分布式拒绝服务攻击，则目标应考虑：

1)向被攻击的服务添加更多本地容量（带宽或服务器）；

2)部署特定于拒绝服务/分布式拒绝服务的基于前提的缓解设备和/或在本地硬件中使用反拒绝服务功能；

3)为其网络运营商，托管提供商或第三方分布式拒绝服务缓解提供商购买基于网络的分布式拒绝服务保护；

4)对于适当的系统，如网站，如果未来发生的攻击会减少攻击的影响，同时仍向客户提供必要或重要的服务，则应制定计划，将站点提供的服务减至最少；

5)与软件和硬件供应商协调，为最佳设备配置提供指导；

6)设计系统捕获攻击流量，攻击IP地址和相应的时间戳；

7)共享捕获的敌对/攻击代码，策略，技巧，攻击来源和向可能遭受类似攻击类型的组织和中央协调组织（例如，US-CERT和NCS / NCC）进行审查，分析和分发给更广泛的受众的程序；和

8)与网络运营商，主机提供商，ISAC或CERT合作，识别攻击的计算机并清理远端的计算机，以最大程度地减少未来攻击的可能性。

BP参考/评论：
阶段：后期系统（目标）
实施指导：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：H

BP号：（从网络运营商部门重复）9-8-8515
更新为：
从滥用或不当使用系统资源中进行恢复：
如果检测到滥用行为或未经授权使用受其控制的系统（例如，检测到参与分布式拒绝服务攻击），则网络运营商，主机提供商或目标应在可行的情况下对系统进行取证分析，验尸分析，应用控制措施防止未来攻击和/或实施系统资源配额。 BP参考/评论：
IETF RFC2350，CMU / SEI-98-HB-001。
阶段：后期服务（网络运营商，托管提供商，目标）
实施指南：　　有效性（H / M / L）：M
　　实施难度：（H / M / L）：H