

# 分布式反射： 新一代的 DDoS 攻击

原著：Steve Gibson [www.grc.com](http://www.grc.com)

翻译：无用君 [www.isfocus.com](http://www.isfocus.com)

译者注：

前几天收到朋友寄来的这篇文章，觉得相当有意思，所以就翻译出来了。因为时间比较紧，我只翻译了原理及防御部分，前面还有一堆关于拒绝服务攻击历史及理论的一堆废话，想看到朋友请去 <http://grc.com/dos/drdoS.htm> 看原文。请不要来跟我们来要 exploit，有心的朋友把那些在网上早已传烂了的 SYN Flood 工具改一改（甚至改都不用改）就可以拿来做这个用了。这篇文章算是给国内的网管敲个警钟吧。

正文：

2002 年一月 11 日凌晨两点，grc.com 被一些更先进的恶意洪水数据包攻击。这种新型的 DDoS 攻击可以被成为**分布式反射拒绝服务攻击 ( Distributed Reflection Denial of Servie Attack ) — DRDoS**

## 神秘的洪水攻击

攻击在凌晨两点左右开始，那时我正好还在工作，所以才有机会迅速的抓取到一部分的洪水攻击的信息。这次攻击使 Verio（我们的网络提供商）的集合路由器将攻击数据挤满了我们的两条 T1。我们的网站服务器因为这次攻击而无法处理其它合法的请求。我们被完全的炸下了网。

我们以前就曾遭受过 UDP 和 ICMP 洪水攻击，这些攻击其实都可以由被攻击者入侵的主机、zombie 工具及 Windows 系统简单的实现，我们也被一些经典的 SYN 洪水攻击过。所以我查看了一下那些显示我们是被 SYN/ACK 数据攻击的攻击数据包后，眉毛跳了一下。毕竟这些事实并不重要，就像我以前说的那样，一个 SYN/ACK 包只是一个 SYN 数据包带了一个 ACK 标记。任何有限权制作"raw socket"的人都可以制作出这种数据包来 —— 不管他是恶意的还是无意的。

## 真正的惊讶是当我看到这些发起攻击的地址：

IP 来源地址	主机名
[REDACTED]	[REDACTED]
129.250.28.1	ge-6-2-0.r03.sttlwa01.us.bb.verio.net
129.250.28.3	ge-1-0-0.a07.sttlwa01.us.ra.verio.net
129.250.28.20	ge-0-1-0.a12.sttlwa01.us.ra.verio.net
129.250.28.33	ge-0-0-0.r00.bcrtfl01.us.bb.verio.net
129.250.28.49	ge-1-1-0.r01.bcrtfl01.us.bb.verio.net
129.250.28.98	ge-1-2-0.r00.sfldmi01.us.bb.verio.net
129.250.28.99	ge-1-0-0.a00.sfldmi01.us.ra.verio.net
129.250.28.100	ge-1-1-0.a01.sfldmi01.us.ra.verio.net
129.250.28.113	ge-1-2-0.r01.sfldmi01.us.bb.verio.net
129.250.28.116	ge-1-1-0.a00.sfldmi01.us.ra.verio.net
129.250.28.117	ge-1-0-0.a01.sfldmi01.us.ra.verio.net
129.250.28.131	ge-0-3-0.a00.scrmca01.us.ra.verio.net

```
129.250. 28.142 ge-0-2-0.r00.scrmca01.us.bb.verio.net
129.250. 28.147 ge-1-2-0.a00.scrmca01.us.ra.verio.net
129.250. 28.158 ge-0-2-0.r01.scrmca01.us.bb.verio.net
129.250. 28.164 ge-1-0-0.a10.dllstx01.us.ra.verio.net
129.250. 28.165 ge-1-0-0.a11.dllstx01.us.ra.verio.net
129.250. 28.190 ge-6-0-0.r01.dllstx01.us.bb.verio.net
129.250. 28.200 ge-0-2-0.a00.snjsca03.us.ra.verio.net
129.250. 28.201 ge-0-2-0.a01.snjsca03.us.ra.verio.net
129.250. 28.221 ge-2-1-0.r04.snjsca03.us.bb.verio.net
129.250. 28.230 ge-1-1-0.a00.snjsca03.us.ra.verio.net
129.250. 28.231 ge-1-1-0.a01.snjsca03.us.ra.verio.net
129.250. 28.254 ge-2-1-0.r01.snjsca03.us.bb.verio.net

205.171. 31. 1 iah-core-01.inet.qwest.net
205.171. 31. 2 iah-core-02.inet.qwest.net
205.171. 31. 5 iah-core-01.inet.qwest.net
205.171. 31. 6 iah-core-03.inet.qwest.net
205.171. 31. 9 iah-core-01.inet.qwest.net
205.171. 31. 13 iah-core-01.inet.qwest.net
205.171. 31. 17 iah-core-01.inet.qwest.net
205.171. 31. 21 iah-core-01.inet.qwest.net
205.171. 31. 25 iah-core-02.inet.qwest.net
205.171. 31. 33 iah-core-01.inet.qwest.net
205.171. 31. 37 iah-core-01.inet.qwest.net
205.171. 31. 41 iah-core-02.inet.qwest.net
205.171. 31. 53 iah-core-02.inet.qwest.net
205.171. 31. 57 iah-core-03.inet.qwest.net
205.171. 31. 61 iah-core-02.inet.qwest.net
205.171. 31. 81 iah-core-03.inet.qwest.net

206. 79. 9. 2 globalcrossing-px.exodus.net
206. 79. 9.114 exds-wlhm.gblx.net
206. 79. 9.210 telefonica-px.exodus.net

208.184.232. 13 core1-atl4-oc48-2.atl2.above.net
208.184.232. 17 core2-atl4-oc48.atl2.above.net
208.184.232. 21 core1-atl4-oc48.atl2.above.net
208.184.232. 25 core2-core1-oc48.atl2.above.net
208.184.232. 45 core1-core2-oc192.sfo1.above.net
208.184.232. 46 core2-core1-oc192.sfo1.above.net
208.184.232. 54 sfo1-sjc2-oc48-2.sfo1.above.net
208.184.232. 57 ord2-seal-oc48-2.ord2.above.net
208.184.232. 58 seal-ord2-oc48-2.seal.above.net
208.184.232. 97 bos2-dca2-oc48.bos2.above.net
208.184.232. 98 dca2-bos2-oc48.dca2.above.net
208.184.232.101 bos2-dca2-oc48-2.bos2.above.net
208.184.232.102 dca2-bos2-oc48-2.dca2.above.net
208.184.232.109 core1-dfw3-oc48.dfw2.above.net
208.184.232.110 core1-dfw2-oc48.dfw3.above.net
208.184.232.113 core2-dfw3-oc48.dfw2.above.net
208.184.232.114 core2-dfw2-oc48.dfw3.above.net
208.184.232.118 core1-dfw1-oc48.dfw2.above.net
208.184.232.126 sfo1-sjc2-oc48.sfo1.above.net
208.184.232.133 dca2-dfw2-oc48-2.dca2.above.net
208.184.232.134 dfw2-dca2-oc48-2.dfw2.above.net
208.184.232.145 ord2-bos2-oc48.ord2.above.net
208.184.232.146 bos2-ord2-oc48.bos2.above.net
208.184.232.149 lgal-ord2-oc48.lgal.above.net
```

208.184.232.150	ord2-lga1-oc48.ord2.above.net
208.184.232.157	atl2-lga2-oc48.atl2.above.net
208.184.232.158	lga2-atl2-oc48.lga2.above.net
208.184.232.165	atl2-lga2-oc48-2.atl2.above.net
208.184.232.166	lga2-atl2-oc48-2.lga2.above.net
208.184.232.177	sjc3-paol-oc12.above.net
208.184.232.189	bos2-lga2-oc48.bos2.above.net
208.184.232.190	lga2-bos2-oc48.lga2.above.net
208.184.232.193	bos2-lga2-oc48-2.bos2.above.net
208.184.232.194	lga2-bos2-oc48-2.lga2.above.net
208.184.232.197	core2-lga2-oc192.lga1.above.net
208.184.232.198	core2-lga1-oc192.lga2.above.net
208.184.233.46	ord2-sjc2-oc48.ord2.above.net
208.184.233.50	core2-sjc2-oc48.sjc3.above.net
208.184.233.61	iad1-lga1-oc192-2.iad1.above.net
208.184.233.62	lga1-iad1-oc192-2.lga1.above.net
208.184.233.65	iad1-lga1-oc192.iad1.above.net
208.184.233.66	lga1-iad1-oc192.lga1.above.net
208.184.233.81	core1-main1colo56-oc48.sea2.above.net
208.184.233.85	core1-main2colo56-oc48.sea2.above.net
208.184.233.89	core2-main1colo56-oc48.sea2.above.net
208.184.233.93	core2-main2colo56-oc48.sea2.above.net
208.184.233.101	core1-core2-oc192.sea2.above.net
208.184.233.102	core2-core1-oc192.sea2.above.net
208.184.233.105	core2-sea2-oc192.sea1.above.net
208.184.233.106	core2-sea1-oc192-2.sea2.above.net
208.184.233.121	core1-core2-oc192.dca2.above.net
208.184.233.126	iad1-dca2-oc192.iad1.above.net
208.184.233.129	dca2-iad1-oc192.dca2.above.net
208.184.233.130	iad1-dca2-oc192.iad1.above.net
208.184.233.134	dca2-sjc2-oc48.dca2.above.net
208.184.233.150	ord2-dfw2-oc48.ord2.above.net
208.184.233.174	globalcenter-above.iad2.above.net
208.184.233.189	seal-nrt3-stml.seal.above.net
208.184.233.190	nrt3-seal-stml.nrt3.above.net
208.184.233.193	seal-nrt3-stml-3.seal.above.net
208.184.233.194	nrt3-seal-stml-3.nrt3.above.net
208.184.233.197	core1-main1-oc12.nrt3.above.net
208.184.233.201	core1-main2-oc12.nrt3.above.net
208.184.233.205	core2-main1-oc12.nrt3.above.net
208.184.233.209	core2-main2-oc12.nrt3.above.net
208.184.233.217	core2-core3-oc48.lga1.above.net
208.184.233.225	core2-v6core3-oc3.nrt3.above.net
208.184.233.237	core1-oc192-core2.bos2.above.net
208.184.233.238	core2-oc192-core1.bos2.above.net
208.185.0.25	core5-dlr-oc3.iad1.above.net
208.185.0.113	core5-main1-oc48.iad1.above.net
208.185.0.117	core5-main2-oc48.iad1.above.net
208.185.0.121	core4-iad4-oc48.iad1.above.net
208.185.0.133	core5-iad4-oc48.iad1.above.net
208.185.0.138	core4-core1-oc48.iad1.above.net
208.185.0.142	core4-core3-oc48.iad1.above.net
208.185.0.146	core5-core1-oc48.iad1.above.net
208.185.0.150	core5-core3-oc48.iad1.above.net
208.185.0.153	core4-main1-oc48.iad1.above.net
208.185.0.157	core4-main2-oc48.iad1.above.net
208.185.0.165	core1-core2-oc48.lga3.above.net
208.185.0.166	core2-core1-oc48.lga3.above.net

208.185. 0.169	core1-lga3-oc12.lga1.above.net
208.185. 0.170	core1-lga1-oc12.lga3.above.net
208.185. 0.173	core1-core3-oc3-2.lga3.above.net
208.185. 0.177	core2-core3-oc3.lga3.above.net
208.185. 0.189	core1-core3-oc48.ord2.above.net
208.185. 0.193	core2-core3-oc48.ord2.above.net
208.185. 0.197	core1-ord1-oc48.ord2.above.net
208.185. 0.202	core2-ord1-oc48.ord2.above.net
208.185. 0.221	core1-core3-oc48.atl12.above.net
208.185. 0.225	core2-core3-oc48.atl12.above.net
208.185. 0.229	dca2-atl12-oc48-2.dca2.above.net
208.185. 0.230	atl12-dca2-oc48-2.atl12.above.net
208.185. 0.233	core1-core2-oc192.lga1.above.net
208.185. 0.234	core2-core1-oc192.lga1.above.net
208.185. 0.237	core1-core3-oc48.lga1.above.net
208.185. 0.245	core1-lga2-oc192.lga1.above.net
208.185. 0.246	core1-lga1-oc192.lga2.above.net
208.185. 0.249	core1-dfw2-oc48.atl12.above.net
208.185. 0.250	core1-atl12-oc48.dfw2.above.net
208.185.156. 2	core2-lhr1-stm16.lhr3.above.net
208.185.156. 65	core3-core5-oc48.sjc2.above.net
208.185.156.121	core2-sea2-oc192-2.sea1.above.net
208.185.156.122	core1-sea1-oc192-2.sea2.above.net
208.185.156.157	ord2-lga1-oc48-2.ord2.above.net
208.185.156.158	lga1-ord2-oc48-2.lga1.above.net
208.185.156.189	core3-main1colo7-oc12.sjc2.above.net
208.185.156.193	core4-main2colo7-oc12.sjc2.above.net
208.185.175. 90	ord2-sea1-oc48.ord2.above.net
208.185.175. 93	core3-core4-oc3.sea1.above.net
208.185.175.114	earthlink-above.lax.above.net
208.185.175.145	core1-core2-oc192.sjc3.above.net
208.185.175.146	core2-core1-oc192.sjc3.above.net
208.185.175.149	core2-sjc4-oc192.sjc3.above.net
208.185.175.158	core1-sjc2-oc48.sjc3.above.net
208.185.175.178	core2-core1-oc48.sea1.above.net
208.185.175.182	core3-core1-oc48.sea1.above.net
208.185.175.189	core1-main1colo56-oc48.sjc3.above.net
208.185.175.193	core1-main2colo56-oc48.sjc3.above.net
208.185.175.197	core2-main1colo56-oc48.sjc3.above.net
208.185.175.201	core2-main2colo56-oc48.sjc3.above.net
216.200.127. 9	core4-iad5-oc48.iad1.above.net
216.200.127. 13	core5-iad5-oc48.iad1.above.net
216.200.127. 26	sjc2-iad1-oc48.sjc2.above.net
216.200.127. 29	core4-epel-oc3.iad1.above.net
216.200.127. 33	core5-epel-oc3.iad1.above.net
216.200.127. 45	core1-epel-oc3.lga1.above.net
216.200.127. 49	core2-epel-oc3.lga1.above.net
216.200.127. 61	iad1-lga1-oc48-2.iad1.above.net
216.200.127. 62	lga1-iad1-oc48-2.lga1.above.net
216.200.127. 65	lga1-sea1-oc48.lga1.above.net
216.200.127. 66	sea1-lga1-oc48.sea1.above.net
216.200.127. 69	lga1-lhr1-stm4-3.lga1.above.net
216.200.127.118	sea1-sjc2-oc48.sea1.above.net
216.200.127.145	core1-core2-oc192.lga2.above.net
216.200.127.146	core2-core1-oc192.lga2.above.net
216.200.127.149	core1-core3-oc48.lga2.above.net
216.200.127.153	core1-main1colo45-oc48.lga2.above.net
216.200.127.157	core1-main2colo45-oc48.lga2.above.net

```
216.200.127.161 core1-main1colo678-oc48.lga2.above.net
216.200.127.165 core1-main2colo678-oc48.lga2.above.net
216.200.127.169 core2-core3-oc48.lga2.above.net
216.200.127.173 core2-main1colo45-oc48.lga2.above.net
216.200.127.177 core2-main2colo45-oc48.lga2.above.net
216.200.127.181 core2-main1colo678-oc48.lga2.above.net
216.200.127.185 core2-main2colo678-oc48.lga2.above.net
216.200.127.189 core1-main1-oc48.lga1.above.net
216.200.127.194 core1-main2-oc48.lga1.above.net
216.200.127.197 core2-main1-oc48.lga1.above.net
216.200.127.201 core2-main2-oc48.lga1.above.net
216.200.127.205 dfw2-dca2-oc48.dfw2.above.net
216.200.127.206 dca2-dfw2-oc48.dca2.above.net
216.200.127.209 core1-core2-oc192.dfw2.above.net
216.200.127.210 core2-core1-oc192.dfw2.above.net
216.200.127.213 core1-core3-oc48.dfw2.above.net
216.200.127.217 core2-core3-oc48.dfw2.above.net
216.200.127.225 atl2-dfw2-oc48.atl2.above.net
216.200.127.226 dfw2-atl2-oc48.dfw2.above.net
```

**我们看起来是在被超过 200 多个网络核心基础设施路由器攻击。**

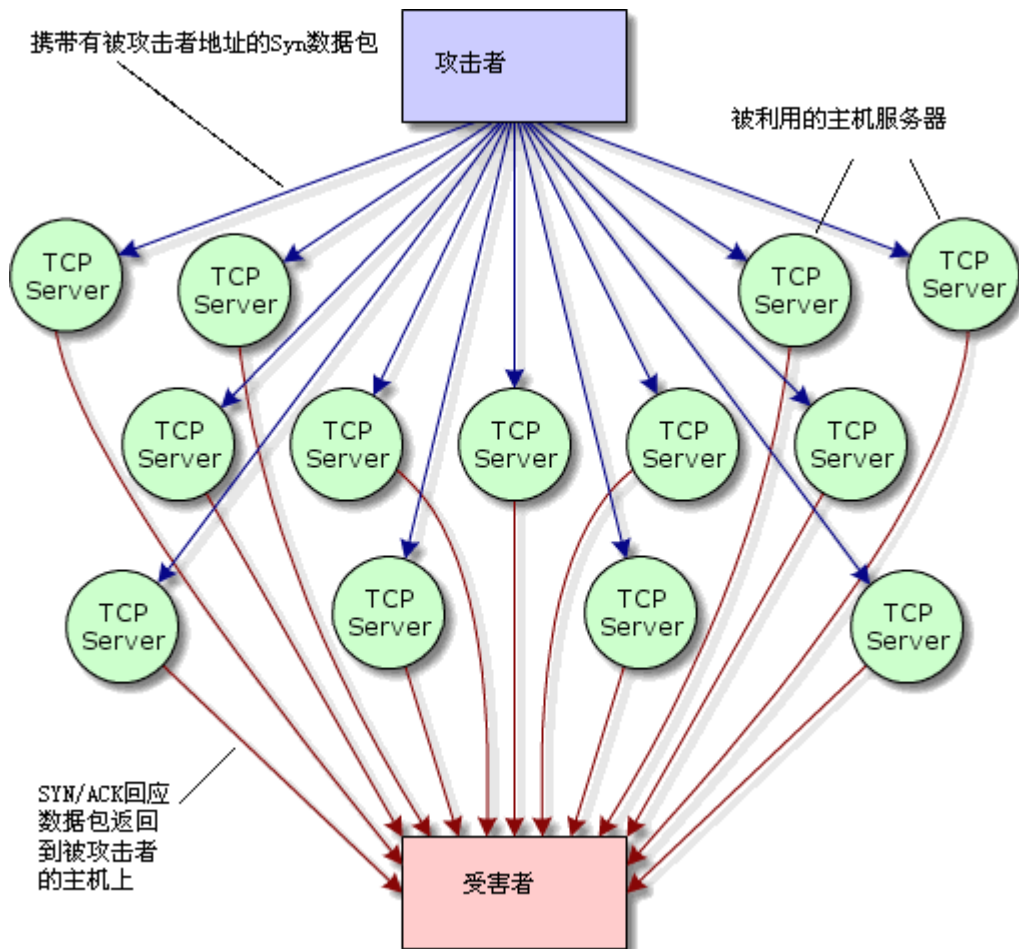
**发生什么事了？**

看到这些分别来自 Verio、Qwest、和 Above.net 的洪水数据包，我想它们都是完全合法的 SYN/ACK 连接回应包，它们显示了一个 TCP 源端口：179。换句话说，就像一个网页服务器的数据包会从 HTTP 的 80 号端口返回一样，这些数据包是从"BGP"的 179 号端口返回的。

BGP 是中介路由器支持的"边界网关协议" (Border Gateway Protocol)。路由器使用 BGP 与他们的邻居进行即时的信息交流来交换他们的"路由表"，这是为了通知它们彼此路由器可以在哪个 IP 范围进行转交。

BGP 的细节并不重要，重要的是每个良好连接（高宽带）的中介路由器都会接受在他们 179 端口上的连接。换句话说，任何一个 SYN 数据包到达一个网络路由器上后都会引出一个该路由的 SYN/ACK 回应包来。

**我突然知道什么会一定发生.....**



这些被用来攻击的两百台主机不可能全存在安全问题，甚至可能没有任何一台有安全问题。我认识到它们只不过全是一些普通的 TCP 服务器，它们是在认为我们想建立一个 TCP 连接到它们自带的 BGP 服务的情况下才向 grc.com 发送 SYN/ACK 数据包的。

换句话说，一个恶意的入侵者在其他的 Internet 角落里利用带有连接请求的 syn 数据包对网络路由器进行洪水攻击。这些数据包带有虚假的 IP 地址，这些地址都是 grc.com 的。这样一来，路由器认为这些 Syn 数据包是从 grc.com 发送来的，所以它们便对它们发送 SYN/ACK 数据包作为三次握手过程的第二个步。

**恶意的数据包其实就被那些被利用的主机“反射”到了受害者主机上。这些被反射的数据包返回到受害者主机上后，就形成了洪水攻击。**

## 阻拦反射攻击

我们有一些好消息，这种攻击看起来可以很简单的阻拦。因为我们自己不是网络服务提供商，以我们从来没有任何连接到远程带有 BGP 服务的路由器上的需要。这样一来，我便要求 Verio 去阻拦任何从 BGP 服务端口 179 发起的入站数据。因为这个恶意攻击者的 SYN 数据包的目标是网络上中介路由的 179 号端口，任何反射的数据包也应该会从这个端口发出。

Verio 的工程师加了一个 filter 到提供我们网络服务的集合路由上，它用来阻拦（丢弃）任何从 179 端口发来的数据包。从 179 号端口发送来的数据包洪水立即停止了。

**但我们并没有回到 Internet 上。**

一个刚从网上抓到的数据包显示我们现在正被一群全新的网络服务器攻击。因为这第二群攻击是在我们阻拦了从 179 端口发送来的攻击以后才出现的，所以这第二拨攻击没有办法跟第一拨的攻击力相比。

我们现在正在被从端口 22 (Secure Shell), 23 (Telnet), 53 (DNS), 和 80 (HTTP/Web) 上发送来的 SYN/ACK 数据包攻击。这其中还有一些从端口 4001 (代理服务器端口)和 6668 (IRC 聊天)发送来的数据包。

很可惜的是，因为这第二波攻击完全出乎我的意料，所以我没有抓到这第二波攻击的完整的数据包来作为取样。不过，我先前在第一波攻击中所抓到一些日志有展现一些非 BGP 所发出的 SYN/ACK 包。

### 这是一小部分先前从 HTTP(网页服务)端口 80 上所发出 SYN/ACK 攻击数据包的样本

IP 来源地址	主机名
██████████	██████████
64.152. 4. 80	www.wwfsuperstars.com
128.121.223.161	veriowebsites.com
131.103.248.119	www.cc.rapidsite.net
164.109. 18.251	whalenstoddard.com
171. 64. 14.238	www4.Stanford.EDU
205.205.134. 1	shell1.novalinktech.net
206.222.179.216	forsale.txic.net
208. 47.125. 33	gary7.nsa.gov
216. 34. 13.245	channelserver.namezero.com
216.111.239.132	www.jeah.net
216.115.102. 75	w3.snv.yahoo.com
216.115.102. 76	w4.snv.yahoo.com
216.115.102. 77	w5.snv.yahoo.com
216.115.102. 78	w6.snv.yahoo.com
216.115.102. 79	w7.snv.yahoo.com
216.115.102. 80	w8.snv.yahoo.com
216.115.102. 82	w10.snv.yahoo.com

这蜂拥而来的 SYN/ACK 数据包和一些非路由的网络服务器告诉了我们，任何用于普通目的 TCP 连接许可的网络服务器都可以用做数据包反射服务器。当我看到我们光阻拦从 BGP 端口传来的数据是远远不够的，我开发了一套更全面的解决方案来对付这种攻击。这套方案我们会在下面讨论。

在装置好对付反射攻击的 filter 后，我们立即就可以重新返回网上了。经过我不可以监控在装置 filter 后的攻击状况，但看到下面的这些信息还是让我冒了一阵冷汗...

### 直到攻击停止，Verio 的路由丢弃了将近十亿(1,072,519,399)的恶意 SYN/ACK 数据包。

我是在认识我到没有抓到第二波非 BGP 的数据包后才联系 Verio，从而得知这个数据的。我想要重新装备我们的防御系统，好让我们继续遭受攻击，这样才能抓到那些我先前没有收集到的资料，但当我这样做的时候，攻击已经停止了。

## 反射攻击的防御及预防

通过 Internet 进行交流的电脑一般都可以被分为两类：客户端及服务端。这两个角色可以随着环境转换（例如一个网页服务器可能会是一个邮件服务器的客户端），不过大部分的 TCP 连接都意味着一个客户端和服务端的关系。客户端一般会从一个高数位的端口发起连接到服务端上处于监听状态的底数位端口上。

因为任何反射的 SYN/ACK 数据包必须要弹到一个 TCP 服务器上，并且因为几乎所有的服务端端口都在 1 到 1023 这个范围之内，阻拦所有在服务端口范围之内入站的数据包会防止大部分的攻击造成的阻塞。不过这样做会产生一些问题.....

### 保护服务器

首先，这次对 grc.com 的攻击包含了从端口 4001 和 6668 来的 SYN/ACK 数据包。所以，如果从这些端口发出的数据太多的话，这些特殊的高数位服务端口也需要被阻拦。在阻拦高数位端口的入站数据包存在一个问题，那就是一些合法的客户端的端口所发生的数据可能也会因为我们设置的 filter 给拦截掉。

第二个问题是如果我们只是简单的拦截所有从 1024 以下端口发送的数据的话，那么像当一个在 blanket filter 后的服务器作为客户端的话，它将无法和其它服务器进行交流。就像我们刚才举的例子一样，当一个网页服务器作为一个 SMTP 服务器的客户端时，这个情况就会变的非常复杂。因为远程 SMTP 服务器的数据包会试图从 SMTP 服务器的 25 号端口返回，这时它就会被我们设置的反反射攻击的 filter 给拦截掉。为了解决这个问题，我们需要在配置文件里设置例外端口，这样才可以让合法数据包正常通过。

### 保护客户端

这里有一些坏消息。客户端主机，例如那些典型的终端用户，将无法被保护。因为多数的客户端在大部分时间里都是连接到远程的服务器端上的，这些服务器端很可能会被利用来攻击这些无辜的客户端。

### 译者注：

国内的网管可能都冒了一身的冷汗，以前的分布式拒绝服务式攻击可以算是可见不可及。毕竟那是需要几百台受控的肉鸡才能实现的，可现在这个技术可以利用任何不存在安全漏洞的主机来进行攻击，后果可以想象。原作者上面所说的利用 filter 来拦截数据包只是暂时之策，服务器不用来提供服务还有屁用？所以真正的解决办法还是要从基础的配置做起，这种攻击不是使用半连接来挂掉主机，所以对付以前那种传统的 SYN Flood 的方法可能无法在这里行通。到目前为止，通过利用防火墙来阻挡那些序列号不对的数据包恐怕是最好的方法了。

希望网络安全界的人士能尽快研究出更好的解决方法。

**另外也请那些能自己悟出 Exploit 的高手不要将攻击方法乱传，以国内现在的安全水准，无法经受起这种攻击，慎思。**