# Compreendendo Ataques *Denial of Services*

**Leandro Márcio Bertholdo, Andrey Vedana Andreoli e Liane Tarouco**

Computer Emergency Response Team of RS – CERT-RS
Centro de Processamento de Dados da Universidade Federal do Rio Grande do Sul
Rua Ramiro Barcelos, 2574 – Porto Alegre – RS – Brasil
{berthold,andrey,liane}@penta.ufrgs.br

***Resumo.***

*Esse trabalho aborda o tópico de ataques de negação de serviço (DoS), inclusive distribuídos (DDoS). Nele são analisados alguns dos ataques clássicos e outros que ainda são utilizados, concentrando-se no que os autores consideram como os mais nocivos desta classe: os ataques distribuídos. São citadas classificações, características e contra-medidas que são utilizadas e/ou pesquisadas em relação à detecção e bloqueio dessa classe de ataques.*

## 1. Introdução

Os ataques conhecidos como denial-of-service (DoS) são caracterizados por uma tentativa explícita do atacante de impedir que um usuário legítimo utilize determinado serviço[CERT 97]. Algumas estratégias utilizadas nesses ataques são:

- Inundar uma rede visando impedir que usuários legítimos façam uso dela.
- Impedir ou romper a conexão entre duas máquinas visando impedir o acesso a um serviço.
- Impedir o acesso de um determinado serviço ou site.
- Impedir ou negar um serviço a um sistema ou pessoa específicos.

Conceitualmente, nem todos os ataques contra serviços são necessariamente ataques de negação de serviço. Em outros casos, alguns tipos de ataques podem incluir um componente de negação de serviço como parte de um ataque maior, como o caso Mitnick [NOR 99].

Os ataques distribuídos possuem conceitos semelhantes aos de sistemas distribuídos, ou seja, são ataques que podem ser efetuados a partir de diversos computadores simultaneamente. Neste tipo de ataque é realizada uma sobrecarga ou inundação de pacotes contra um determinado serviço, host ou rede, gerando muitas vezes uma quantidade de dados global maior que a rede ou host pode suportar, tornando a rede ou serviços instáveis e conseqüentemente prejudicando o seu desempenho [NEU 99] [CERT 00].

Segundo estatísticas do CERT/CC [CERT 01], vários ataques DoS e DDoS são registrados diariamente, e envolvem principalmente novos vermes e ferramentas para DDoS. Alguns desses vermes incluem um comando e estrutura de controle que permite ao intruso dinamicamente modificar o comportamento do verme após ele infectar a

vítima. Em alguns casos esse controle é inclusive realizado sem que o atacante necessite saber quem são os sistemas que foram infectados – foram registrados casos onde o host infectado monitora um canal IRC aguardando a ordem para atacar. Características como essa tornam ainda mais difícil desenvolver uma solução global para o problema. Ferramentas como essa possuem somente um objetivo: terrorismo.

## 2. Características

Os ataques de denial-of-service surgiram explorando falhas de implementação em serviços e sistemas operacionais, como Ping-of-dead[1] [CERT 96] e, em alguns casos, até mesmo a forma de funcionamento dos protocolos, como no caso do SYN Flooding[2] [CERT 96b] e do UPD packet storm[3] [CERT 96c]. Em um segundo momento, surgiram os amplificadores de ataque, tais como os ataques smurf[4] [CERT 98] utilizando técnicas de IP Spoofing [CERT 95].

Com o passar dos anos todas as técnicas de ataques conhecidas (spoofing, flooding, amplificadores de ataques, etc.) acabaram por ser incorporadas nos ataques DoS, e esses, por sua vez, realizados de forma distribuída. Para se chegar a esse nível de contaminação, o conceito utilizado foi o de vermes e viroses, através do qual uma vulnerabilidade explorada na máquina do usuário injeta um código malicioso que aguarda as ordens do atacante sobre o alvo a ser atingido e os ataques a serem realizados. Em muitos casos antigas ferramentas como Trinoo, TFN e Mstream [CERT99][CERT 99b] em novas formas utilizadas, acrescidas do requinte de trocar as informações de ataque de forma cifrada.

## 3. Ferramentas utilizadas para realizar ataques DoS e DDoS

Basicamente o ataque DDoS caracteriza-se por, primeiramente, explorar vulnerabilidades já conhecidas em sistemas operacionais e serviços e, através delas, obter acesso privilegiado a qualquer máquina na Internet. Geralmente esse acesso indevido é obtido através de scripts automatizados que varrem toda a Internet a procura de hosts vulneráveis. No passado, quando as ferramentas para DDoS eram instaladas manualmente, a preferência era por hosts bem conectados e sistemas operacionais que permitissem a instalação de sniffers e rootkits. Hoje em dia, com o advento de conexões domésticas de banda larga (ADSL, Cable, ISDN) essa preferência não existe mais.

---

[1] O ping-of-death era caracterizado por gerar um buffer overflow quando o host atacado recebia um pacote ICMP de tamanho superior a 65535 bytes, causando uma reinicialização ou desativação do sistema operacional do host atacado.

[2] Nesse caso o host era atacado com inúmeras tentativas de estabelecer uma conexão para um serviço (pacotes SYN) e não aceitava novas conexões até obter uma resposta das que estavam nesse estado. Essa resposta nunca era enviada e as conexões somente recebiam um timeout após alguns minutos – mas o atacante enviava constantemente outros pedidos de conexão.

[3] Uma das formas desse ataque faz uso da porta udp/echo, que faz com que o host solicitado envie indefinidamente e na maior velocidade possível pacotes para a estação solicitante.

[4] O ataque smurf se aproveita da existência de um endereço de broadcast direto, que permite que uma estação remota solicite uma resposta de todas as estações em uma determinada rede. Como o atacante forja o endereço da estação conectada e emite um fluxo constante de requisições, um único pacote enviado pelo atacante pode facilmente ser multiplicado por 100 vezes ou mais.

Depois de realizado esse primeiro passo, a invasão do sistema, e considerando-se as versões originais do TFN e Trinoo, uma lista de endereços IPs das máquinas exploradas formam a rede de ataque. Neste ponto, cada uma das máquinas listadas já possui instalado o software necessário para efetuar o ataque propriamente dito, ou seja, as ferramentas para DoS.

No passo seguinte é criada uma hierarquia de ataque, composta pelos atacantes, estações mestres e estações zumbis. As máquinas consideradas mestres eram responsáveis por receberem os comandos de ataque, reenviando-os às estações zumbi. Este grupo de zumbis era quem efetivamente concretizava o ataque.

Uma vez que o software estivesse instalado nos futuros zumbis, eles passavam a anunciar ao mestre a sua presença. Assim, para efetuar o ataque bastava que o mestre fornecesse o IP a ser atacado e o tempo que duraria o ataque. A partir desse ponto o zumbi entrava em atividade. Uma conseqüência comum desse ataque era a saturação do link ou a paralisação dos serviços oferecidos pela vítima através de técnicas como SYN Flooding, Smurf ou simplesmente pacotes ICMP destinados à vítima. Veja abaixo a ilustração de uma rede de ataque:

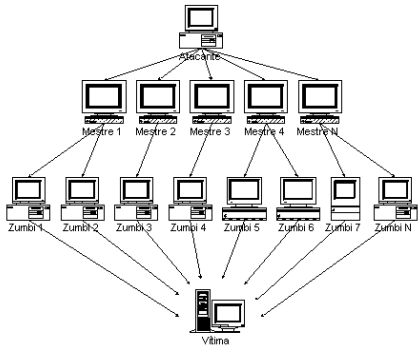



**Figura 1 - Exemplo de rede de ataque para DDoS**

## 4. Evoluções dos Ataques DoS

Nos últimos anos, vermes com um forte potencial nocivo do ponto de vista de negação de serviço foram identificados. Vermes cujo problema gerado foi a sobrecarga na infra-estrutura da rede, tanto no que tange a utilização de cpu de roteadores e switches quando na utilização da banda disponível, sem citar-se o grande número de hosts contaminados e um tempo muito curto [NEU00][CER03][CER03b].

Dentre esses podemos citar o Codered-v2 que em menos de 24h contaminou aproximadamente 350 mil hosts e o W32.Slammer que em 25 de janeiro de 2003 contaminou 75 mil hosts em aproximadamente 30min [CAI 02]. Em ambos os casos vários nodos da rede caíram devido à alta utilização de CPU, e o restante sofreu devido à massiva utilização da rede. Para se ter uma idéia do impacto e do número de redes envolvidas pela ação do W32.Slammer, a figura 2 abaixo mostra a oscilação das tabelas de roteamento BGP de alguns dos maiores provedores mundiais.

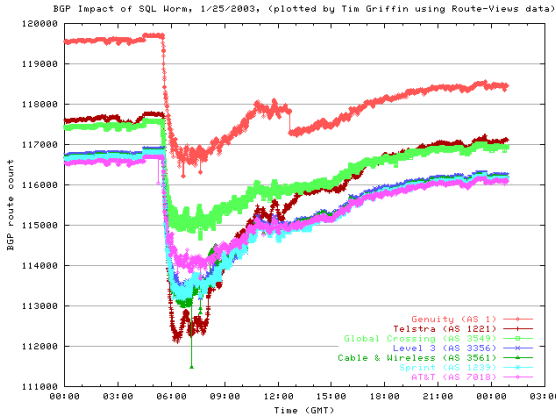
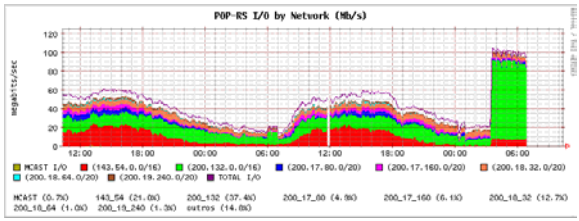



**Figura 2: Impacto no protocolo BGP durante a ação do Slammer**

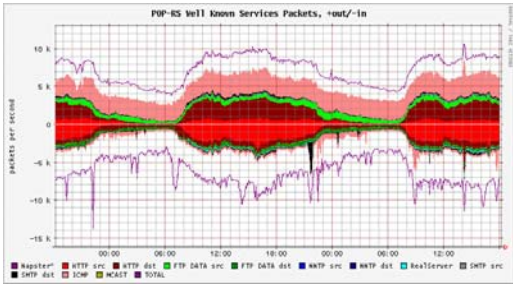
## 5. Como detectar um ataque DoS

Algumas anomalias podem sinalizar a ocorrência deste tipo de ataque, tais como :

- Excesso de tráfego: A banda utilizada excede o máximo, ultrapassando o número de acessos esperados ou a assimetria deste.




- A existência de pacotes UDP e ICMP de tamanho acima do normal ou em excesso: Geralmente as sessões UDP utilizam pacotes pequenos de dados dificilmente maiores que 10 bytes (payload). As mensagens ICMP não excedem a faixa entre 64 e 128 bytes. Pacotes cujo tamanho seja superior a esses números são considerados suspeitos de conter mensagens de controle, destinadas a cada um dos agentes que está participando do ataque. Apesar do conteúdo dos pacotes estar cifrado, o endereço do destino é verdadeiro, desta forma pode-se localizar um dos agentes que estão realizando o ataque baseado no seu fluxo de mensagens.




- Pacotes TCP e UDP que não fazem parte de uma conexão: Alguns tipos de DDOS utilizam aleatoriamente vários protocolos (incluindo protocolos orientados a conexão) para enviar dados sobre canais não orientados a conexão. Isto pode ser detectado utilizando-se firewalls que mantenham o estado das conexões (statefull-firewalls). Outro ponto importante é que estes pacotes costumam destinar-se a portas acima de 1024.

## 6. Contra-medidas

Até o momento, não existe uma solução definitiva contra os ataques de denial-of-service e ataques distribuídos. Algumas pesquisas estão sendo realizadas propondo soluções para peças do problema, como:

- Identificar a origem dos pacotes forjados [BEL 00].
- Inibir os amplificadores de ataques [CERT 98].
- Overlay networks [KER 02].
- Active Networks [STE 02].

## 7. Conclusões

Cabe a cada administrador controlar os recursos de sua rede, observando de forma contínua os comportamentos considerados suspeitos, enumerados anteriormente. Como foi visto, boa parte das tentativas de DOS e DDOS baseiam-se na exploração de vulnerabilidades de onde origina o ataque e pela falta de monitoração e aplicação de ações rápidas por parte de quem sofre o ataque. Uma vez que ambos os lados façam o seu "dever de casa", muitos ataques poderão ser evitados e/ou rapidamente minimizados.

## 7. Referências

[BEL 00] S. Bellovin, "ICMP traceback Messages" Internet Draft, http://www.research.att.com/~smb/papers/draft-bellovin-itrace-00.txt Acesso em Agosto/2003.

[CAI 02] Analysis of the Sapphire Worm http://www.caida.org/analysis/security/sapphire/ Acesso em Agosto/2003.

[CERT 95] CERT® Advisory CA-1995-01 IP Spoofing Attacks and Hijacked Terminal Connections. http://www.cert.org/advisories/CA-1995-01.html Acesso em Agosto/2003.

[CERT 96] CERT Advisory CA-1996-26 Denial-of-Service Attack via ping http://www.cert.org/advisories/CA-1996-26.html Acesso em Agosto/2003.

[CERT 96b] CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks. http://www.cert.org/advisories/CA-1996-21.html Acesso em Agosto/2003.

[CERT 96c] CERT Advisory CA-1996-01 UDP Port Denial-of-Service Attack. http://www.cert.org/advisories/CA-1996-01.html Acesso em Agosto/2003.

[CERT 97] Denial of Service Attacks. CERT Coordination Center . . Outubro/1997 - Initial Release. http://www.cert.org/tech_tips/denial_of_service.html Acesso em Agosto/2003.

[CERT 98] CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks. http://www.cert.org/advisories/CA-1998-01.html Acesso em Agosto/2003.

[CERT 99] Results of the Distributed-Systems Intruder Tools Workshop. Pittsburgh, Pennsylvania USA, November 2-4, 1999.

[CERT 99b] CERT® Advisory CA-1999-17 Denial-of-Service Tools. http://www.cert.org/advisories/CA-1999-17.html Acesso em Agosto/2003.

[CERT 01] CERT Advisory CA-2001-20 Continuing Threats to Home Users. http://www.cert.org/advisories/CA-2001-20.html Acesso em Agosto/2003.

[CERT 03] Advisory CA-2003-08 Increased Activity Targeting Windows Shares. http://www.cert.org/advisories/CA-2003-08.html. Acesso em Agosto/2003.

[CERT 03b] Vulnerability Note VU#484891 - Microsoft SQL Server 2000 contains stack buffer overflow in SQL Server Resolution Service. http://www.kb.cert.org/vuls/id/484891 Acesso em Agosto/2003.

[KAS 02] Kashiwa, Dai; Chen, Eric; Fuji, Hitoshi. Active Shaping: A countermeasure against DDoS Attacks. Universal Multiservice Networks, 2002. ECUMN 2002. 2nd European Conference on. IEEE.

[KER 02] Keromytis, Angelos; et al; SOS: Secure Overlay Services. ACM SIGCOMM, 19-23 Agosto 2002.

[NEU 00] Peter G. Neumann. Inside Denial-of-Service Attacks. Communications of the ACM; April 2000/Vol. 43, No. 4.

[NOR 99] NORTHCUTT, S. 1999. Network Intrusion Detection: An Analyst's Handbook. New Riders.

[STE 02] Sterne Dan; et al; Active Network Based DDos Defense. DARPA Active Networks Conference and Exposition 2002. IEEE Computer Society.