Os ataques DDoS e os reflexos penais informáticos

Com o desenvolvimento da Rede Mundial de Computadores e o aperfeiçoamento dos conhecimentos tecnológicos dos *hackers*, os ataques DDoS (*Distributed Denial of Service*) tornaram-se mais freqüentes na Internet. Os ataques DDoS, mais conhecidos como ataques de negação de serviços distribuídos consistem-se basicamente em impedir o normal funcionamento de determinado serviço na Internet, evitando que os usuários legítimos acessem aquele sistema.

A advogada argentina MARÍA KARINA ARRECHE entende que "*este bloqueo, produce un 'embotellamiento' de información con el consecuente agotamiento de las memorias de las máquinas atacadas, afectando así una parte o la totalidad del funcionamiento de la página.*" [1]

Sem embargos, os ataques de negação de serviços distribuídos iniciam-se com a invasão de computadores que se encontram desprotegidos, com o auxílio de um *cavalo-de-tróia* [2] que com isso, instala no equipamento invadido um programa "*zumbi*" [3]. Assim, com o dia do ataque já pré-determinado, o agente envia remotamente pequenos pacotes de dados com orientações para os computadores que foram "*escravizados*", que obviamente, são feitos sem o consentimento dos proprietários.

Dessa forma, os "*escravos*" obedecem aos comandos do agente e passam a solicitar grande quantidade de informações aos servidores. Como os endereços para o retorno destas informações foram falsificados, o sistema tenta enviar a resposta, mas sem sucesso. Esse procedimento evita que os usuários legítimos sejam atendidos pelo servidor e com a sobrecarga de informações, o servidor é paralisado. [4]

A mestre em ciência da computação SUZANA BEATRIZ DE MIRANDA STRAUCH observa que há uma certa facilidade na execução dos ataques, visto que os sistemas atuais oferecem essa possibilidade, e salienta inclusive que o:

"*Denial of Service não é um ataque propriamente dito, é um tipo de ataque, o qual inclui ataques como sobrecarga da rede, excessivos pedidos de abertura de conexão (SYN Flooding) etc. Os antigos mainframes tinham defesas contra estes ataques, os sistemas atuais são excessivamente pobres em relação a estes ataques. A situação vem piorando com as novas linguagens e ambientes de programação, as quais é possível alocar recursos sem maiores limitações. Java e Javascript são dois bons exemplos, elas podem manipular com bastante liberdade diversos recursos do sistema, possibilitando assim diversas denial of service.*" [5]

Inúmeras são as conseqüências causadas pelos ataques DDoS às empresas de comércio eletrônico. A perda de potenciais negócios e clientes que têm suas tentativas de acesso ao site frustradas é uma delas. Em janeiro de 2000, o *hacker* canadense Mafiaboy provocou prejuízos na ordem de 1,7 bilhão de dólares aos sites Yahoo!, CNN, ZDNet e Amazon [6]. Não obstante a isso, a empresas também têm a sua imagem pública lesada.

Outro fator que contribui com o sucesso dos ataques é a incorreta configuração dos sistemas de segurança dos sites. Segundo o portal *Attrition.org* no ano de 2000 foram registrados cerca de 563 sites

desconfigurados, sendo que para 1999, apenas 124 [7].

No ordenamento jurídico brasileiro não se verifica nenhuma norma que tipifique os ataques DDoS. Tramita no Congresso Nacional – e atualmente encontra-se na Comissão de Educação (juntamente com o PL 84/1999) – o Projeto de Lei n.º 76/2000 de autoria do Senador Renan Calheiros, que traz a tipificação em seu artigo 1.º, *in verbis*:

"*Art. 1.º Constitui crime de uso indevido da informática:*

§ 1.º Contra a inviolabilidade de dados e sua comunicação:

[…]

V – A programação de instruções que produzam bloqueio geral no sistema ou que comprometam a sua confiabilidade."

Sustenta o Senador na fundamentação do Projeto, que:

"*A tipificação desse tipo de delito pelas legislações de todos os países é medida urgente e que não pode esperar mais. Como afirmativa disso tivemos recentemente a invasão dos principais "sites" da rede mundial de computadores "INTERNET", que sofreu ação dos chamados "hackers" ou piratas cibernéticos. Essa ação, embora não tenha chegado atingir diretamente aos consumidores, impediu a oferta de serviços, pois tiraram os sites do ar.*"

Com o atual Código Penal, datado de 1941, é possível punir o agente responsável apenas em razão dos prejuízos advindos com o ataque. O artigo 163, dispõe que todo aquele que "*destruir, **inutilizar** ou deteriorar coisa alheia*", poderá sofrer uma pena de detenção, de 1 (um) a 6 (seis) meses, mais multa. Assim, uma vez comprovado o dano causado por força da *inutilização da network* [8], além da responsabilização criminal, poderá o agente também sofrer punições no âmbito cível, tendo que indenizar a vítima por todos os prejuízos causados.

Entretanto, mais importante do que um remédio jurídico que vise minimizar os prejuízos proporcionados por um ataque dessa natureza, é de substancial importância prevenir a realização desses ataques por meio de mecanismos eficazes de segurança, com o objetivo de manter a integridade dos dados e informações disponíveis na *network* e garantir o normal funcionamento dos serviços.

Há algum tempo atrás, os gastos com a segurança do sistema eram vistos como despesas supérfluas e desnecessárias. Hodiernamente, no entanto, têm se falado em *Return Over Investiment* (ROI), ou seja, no retorno do investimento em segurança. Para o consultor CARLOS CARUSO, "*isso fica evidenciado na análise de riscos, uma vez que o que se pode gastar com segurança, pode significar muito pouco em relação ao risco de perda financeira ou quebra da imagem da empresa, o que pode até acarretar a sua extinção.*" [9]

Contudo, torna-se imprescindível que as empresas e organismos façam uso de recursos *tangíveis* (infra-estrutura, *software*, *hardware*) e *intangíveis* (elementos éticos e legais) de segurança [10], evitando-se, com isso, a obstrução do fluxo normal dos dados e informações no sistema.

No ambiente virtual, os atos ilícitos são produzidos com a mesma facilidade que no ambiente real [11]. Ao pretender tutelar o bem jurídico do cidadão, o Direito deve necessariamente acompanhar toda essa evolução, a fim de possibilitar tal garantia. Somente assim, poderá se falar na utilização (com responsabilidade), dos recursos que a Internet em sua totalidade oferece.

Notas de rodapé:

[1] Internet y el bloqueo de servicios (o “denial of service attack”). In: ZARICH, Faustina. *Derecho Informático*. Buenos Aires: Editorial Juris, 2000, p. 60.

[2] Também conhecidos como *Trojans*.

[3] Os *programas escravos* mais utilizados são o *Tribal Flood Network* e o *Trinoo* que podem ser facilmente obtidos na própria Internet.

[4] Internet gratuita facilita ação de hacker. Jornal **Folha de S. Paulo**, edição de 09.03.2000, p. 02.

[5] STRAUCH, Suzana Beatriz de Miranda. **Aspectos de segurança no protocolo IP**. Porto Alegre: PPGC da UFRGS, 1999, p. 34.

[6] GREGO, Maurício. *Hackers: como eles atacam*. **Revista Info Exame**, nº 179, fevereiro de 2001, p. 39.

[7] GREGO, M. **Obra citada**, p. 35.

[8] *Network* é o conjunto formado por dois ou mais computadores ligados de forma a permitir a transmissão de dados entre eles. A Internet é a maior delas. *Vide* BIANCHI, Adriano Smid. **E-dictionary** . São Paulo: Edicta, 2001, 176.

[9] CARUSO, Carlos. Segurança da informação: fatores de risco e soluções possíveis. **Revista Proteger**, Ano VI, n. 33, Maio/Junho, 2001, p. 60.

[10] LEITE, Celso H. **Segurança na Internet: aspectos legais**. Curso de Extensão Universitária. São Paulo: FECAP – Brasiliano & Associados, 2001.

[11] PINHEIRO, Reginaldo César. Os crimes virtuais na esfera jurídica brasileira. **Boletim do Instituto Brasileiro de Ciências Criminais**, ano 8, nº 101, abril de 2001, p. 19.

Date Created
11/08/2002