História

# Considerações Iniciais

Ataques de negação de serviços existem desde o surgimento das redes de computadores, mas eles não recebiam muita importância até atingirem provedores de serviços de Internet, grandes empresas e órgãos do governo. Com o uso crescente da Internet, obteve-se acesso aos servidores dessas entidades e os ataques tomaram maior visibilidade. Isso atraiu mais pessoas interessadas e métodos cada vez mais sofisticados foram sendo desenvolvidos. Além disso, a defesa a ataques de negação de serviço se tornou um tópico de pesquisa de relevância crescente. A seguir, estão alguns dos principais casos desses ataques.

# Décadas de 80 e 90: Primeiros ataques

Em setembro de 1996, um ataque DoS do tipo *SYN Flood* derrubou o provedor de serviços de Internet de Nova Iorque, Panix, por uma semana, e ataques subsequentes derrubaram também os servidores do *Internet Chess Club* e do jornal *The New York Times*. Dois meses mais tarde, iniciou-se a venda do primeiro produto para proteção a ataques DoS. Esse *software* detectava pacotes SYN recebidos e reiniciava as conexões caso o tráfego recebido pelo computador fosse maior que um limite estabelecido. No entanto, esse programa não impediu um novo ataque do mesmo tipo no servidor principal da Webcom, deixando vários *websites* comerciais fora do ar.

Em janeiro de 1997, um adolescente usou uma combinação de *SYN Flood* com o envio de *pings* a uma taxa muito alta para atacar vários provedores de serviços de Internet na Noruega, na Romênia, no Reino Unido e nos Estados Unidos. Cada vez que os servidores reiniciavam, ele obtinha acesso de administrador, deletava arquivos e cancelava contas dos usuários.

Em janeiro do ano seguinte, várias redes IRC receberam os primeiros ataques *Smurf*. No mesmo mês, um adolescente de Israel lançou vários ataques de DoS direcionados ao Pentágono, à NASA, a vários sistemas de rede militares dos Estados Unidos e a centenas de universidades. O *hacker* usou os ataques Teardrop e Bonk, que exploram vulnerabilidades dos sistemas Windows.

Em 1999, foi executado o primeiro ataque DDoS de destaque: *trinoo* (também conhecido como *trin00*). O ataque foi direcionado à Universidade de Minnesota em agosto de 1999, durou dois dias e envolvia o envio de uma quantidade maciça de pacotes UDP, originados de milhares de computadores. Era usada uma ferramenta de mesmo nome, disponível para Linux e Solaris. Em 2000, surgiu uma versão para Windows, chamada de *wintrinoo*.

# De 2000 a 2004: Ataques se tornam mais frequentes

Em fevereiro de 2000, um jovem de 15 anos do Canadá, apelidado de “Mafiaboy”, executou um ataque de DDoS contra vários *sites* de grandes companhias, incluindo Yahoo (o mais popular serviço de buscas da época), eBay, Amazon, CNN e Dell. O ataque teve uma taxa de envio de dados máxima de 1 GB/s, muito alta para a época, causando prejuízos financeiros de aproximadamente 1,7 bilhão de dólares. “Mafiaboy” foi condenado em setembro de 2001.

O primeiro ataque de negação de serviços usado como protesto foi realizado em julho do mesmo ano, por um consumidor frustado com os serviços das companhias BT, BTInternet e Gameplay.

Em 2001, o incidente mais famoso de segurança de redes de computadores foi um verme (*worm*) programado na China, o *Code Red*. Ele atingiu 250.000 computadores em nove horas. Todos os computadores infectados foram programados para lançar um ataque de negação de serviço ao *website* da Casa Branca. A Casa Branca foi forçada a alterar seu endereço IP e solicitou ao Pentágono que ele tirasse seus *websites* do ar temporariamente. O prejuízo estimado é de 2,6 bilhões de dólares.

Nesse mesmo ano, ocorreu um dos primeiros ataques com motivações políticas, onde sites de órgãos do exército norte-americano sofreram ataques de DoS. O episódio que motivou esses ataques foi a presença de um avião de espionagem dos EUA estava em uma missão de reconhecimento em território chinês. Vários caças chineses o interceptaram, e um deles colidiu com o avião americano. O piloto chinês morreu, e o avião americano teve de fazer um pouso de emergência. A tripulação foi forçada a ficar na China por vários dias. Esse episódio causou tensões entre Estados Unidos e China, motivando os ataques aos servidores americanos. Acredita-se que o grupo chinês *Honker Union* seja o responsável pelos ataques.

Em outubro de 2002, os servidores raiz do DNS (*Domain Name Service*) receberam ataques durante uma hora, e vários ficaram indisponíveis para receber tráfego vindo da Internet. Os servidores que não foram derrubados garantiram que o desempenho da Internet não sofresse grandes consequências, logo um usuário comum dificilmente notou alguma alteração no serviço. No entanto, esse foi o ataque mais sério direcionado a um componente essencial da Internet.

# De 2004 a 2009: novas tendências

Com o público cada vez mais consciente de medidas de segurança e os ataques de DoS cada vez mais direcionados a grandes empresas, informações de ataques de negação de serviço passaram a ser menos ao grande público, pois esses ataques poderiam prejudicar a reputação das empresas. Dessa forma, surgiram como tendências nesses ataques a extorsão e exércitos de *bots*. Além disso, vários ataques de DoS passaram a ser realizados como forma de mobilização política.

Um exemplo de extorsão ocorreu em janeiro de 2006: a “página de um milhão de dólares” (*The Million Dollar Page*), criada pelo estudante britânico Alex Tew para arrecadar dinheiro para a sua formação universitária, sofreu um ataque. O estudante, inicialmente, vendia cada pixel da página por 1 dólar para anúncios, e a página era formada 1 milhão de pixels distribuídos numa grade de 1000 x 1000 pixels. Como a página se tornou um fenômeno na Internet, causando uma febre de compra de pixels, ela recebeu a atenção de vários *hackers*, que executaram ataques de DoS na página, pedindo US$ 5000 e depois US$ 50000 para que eles parassem os ataques. A página recebeu ataques por 1 mês.

Vários grupos de ciber criminosos começaram a se especializar em criar exércitos de bots, tomando o controle de milhares e até milhões de computadores, que eram alugados para interessados em executar ataques de DDoS. Um dos casos mais notórios é o de um “*botmaster*” de 20 anos, que foi condenado a 5 anos de prisão em maio de 2006 por controlar meio milhão de computadores.

Nesse período, também passaram a ocorrer com mais frequência ataques com motivações políticas. Um desses ataques ocorreu em abril de 2008, direcionado ao site da CNN. O jornalista Jim Cafferty havia comentado sobre as preparações dos chineses para as Olimpíadas de Pequim. Muitos chineses consideraram os comentários ofensivos, e isso gerou motivação para ataques virtuais à CNN. Vários grupos de *hackers* se coordenaram para executar vários tipos de ataques, como *defacement* (alterações na aparência de uma página *web*) e negação de serviço. Várias ferramentas para atacar os servidores da CNN foram desenvolvidas para computadores com Windows, além de várias *botnets* com esse objetivo. A primeira ferramenta foi chamada de “Supper DDoS” e era uma ferramenta de ataques de *flood* (inundação) com interface gráfica simples, para que qualquer usuário pudesse executá-la. Na sua interface, só haviam um campo para o endereço IP da vítima e dois botões para iniciar e parar o ataque.

# Dias Atuais

Nos últimos tempos tem se intensificado o uso de botnets para a realização de atividades ilícitas das mais variadas, tais como: DDoS, roubo de dados, armazenamento de dados ilícitos (torrents), etc. Devido ao grande número de usuários sem conhecimento básico em segurança de informação e ao contingente cada vez maior de banda de rede disponível, essas redes têm se tornado cada vez mais um risco potencial para o mercado financeiro, governos, empresas e aos próprios usuários da Internet. Esses ataques podem ocorrer por diferentes motivações e seus agentes podem ser os mais variados. Ataques realizados contra a VISA e a MasterCard em 2010, por exemplo, pelo grupo Anonymous, que se denomina um grupo ativista hacker, tiveram como justificativa uma represália à interrupção do serviço de doações dessas companias ao site WikiLeaks, responsável pela divulgação de documentos secretos de empresas e governos com o intuito de gerar uma maior transparência na estrutura de governança global.

Grupos que praticam ciber terrorismo preocupam cada vez mais os governos e ganharam uma maior visibilidade na mídia nos últimos tempos. Esta preocupação ficou clara com a oferta de recompensa de 3 milhões de dólares por informações sobre o paradeiro do ciber criminoso Evgeniy Mikhailovich Bogachev [1]. Evgeniy Bogachev é responsável pela idealização e desenvolvimento da botnet Gameover Zeus que contaminou cerca de 500.000 computadores ao redor do mundo. Esta botnet tinha como objetivo roubar dados confidenciais para a sua possível venda em mercados negros, como a venda de cartões de créditos existente na Deep Web. Estima-se que os danos gerados por esse criminoso com essa aplicação foram em torno de 100 milhões de dólares [2].

Referências usadas:

[34] Jose Nazario, *Politically Motivated Denial of Service Attacks* - Arbor Networks. Obtido em <https://ccdcoe.org/publications/virtualbattlefield/12_NAZARIO%20Politically%20Motivated%20DDoS.pdf>

[40] Georgios Loukas, Gulay Oke, *Protection Against Denial of Service Attacks: A Survey* - The Computer Journal 53. Obtido em: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.363.3133&rep=rep1&type=pdf>

##### **[41] Phillip Boyle, *Intrusion Detection FAQ: Distributed Denial of Service Attack Tools: trinoo and wintrinoo* - SANS Institute**