Quero comprar um ataque de negação de serviços

No Brasil, muitas pessoas ainda crêem que um ataque a um serviço web é extremamente difícil e somente crackers especializados podem fazê-lo. Esta não é a realidade. Os ataques de negação de serviço, também chamados de DOS (Denial of Service) vem crescendo no mundo e no país, não somente como uma arma de cyberguerra, mas principalmente, como artifício nas mãos de empresas desonestas e como arma para concorrência desleal.

O ataque, apresenta sua variante "distributed", onde inúmeros computadores são utilizados para uma abordagem em servidores e sites de empresas e pessoas alvos, que diante das inúmeras requisições e congestionamento dos serviços suportados, passam a negar demais solicitações. Em síntese, o serviço sai do ar. O ataque foca principalmente o elemento disponibilidade da informação, um dos escopos da segurança informacional, com conseqüente quebra de contratos e dano reputacional à empresa atacada.

Agora, se você pensa que este ataque é somente inerente a guerras internacionais e crackers ideológicos, se engana. Quanto valeria ver um concorrente fora do ar por algumas horas? E é exatamente esta motivação repugnante que nos chamou a atenção para novos serviços disponíveis no mundo cracker. A contratação de um ataque de negação de serviços. Se você pesquisar agora no Google *"want to buy ddos attack" ou "rent DDoS Botnet"* poderá se surpreender com o encontrado.

Criminosos digitais agora oferecem seu portfólio de serviços, o que é assustador, com técnicas que vão de Javascript Attack ou Attack through Scripting a DDOS, que podem ser encomendados

de acordo com os bytes programados, tempo do ataque e perfil das empresas envolvidas. Se você é um criminoso digital de menor porte, também pode comprar no “atacado”, alugando uma Botnet para oferecer serviços a seus clientes!

Os bandidos já estruturam suas redes de ataque, que são utilizadas para produzir o volume de tráfego suficiente para derrubar empresas e serviços dos mais variados portes. Quanto maior o tráfego disparado e zumbis envolvidos, maior será o pagamento. Os serviços não garantem êxito, mas penso que ninguém aqui queira pagar para ver uma “brincadeira” desta natureza em face de seus negócios.

Sabe o que é pior? Os computadores e o tráfego da sua empresa, mesmos sem você saber, podem estar servindo de ativo para o crime digital, passivamente aguardando uma ordem remota, sendo que você poderá ser responsabilizado por isso. Talvez agora você entenda a importância de um teste de stress em sua rede, de intrusões, dimensionamento da capacidade ou análise de vulnerabilidades.

Se oferecer este serviço ainda orbita em uma zona legal cinzenta, a execução do ataque, se comprovada pela perícia digital, ainda que não consumada ou impedida pela equipe de resposta a incidentes, no Brasil, pode ensejar a punição dos responsáveis pelo crime de dano (ainda que tentado), previsto no artigo 163 do Código Penal Brasileiro. Sem prejuízo, se comprovado, os executores e mandante poderão responder pelo crime de concorrência desleal, previsto no art. 195 da Lei 9279/1996. Fica o alerta.