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.

Multa de trânsito online é arma para golpe digital

Em época de licenciamento e IPVA, um e-mail que utiliza o nome do Departamento de Estadas e Rodagem de São Paulo (DER) voltou a circular pela rede nesta semana. Pelo e-mail, enviado de "debitos@der.com.br", enviado em 18/01/2011 às 19h03min, com o assunto "Notificação urgente de multas registradas em nosso SIER", o usuário é levado a acreditar que existem multas registradas para seu veículo, e é induzido a clicar em três links que "supostamente" exibiriam as Notificações de Multa.

Pela mensagem, *"Consta em nosso (SIER) Sistema Integrado de Estradas e Rodagens, várias infrações cometidas pelo seu veículo, e devido ter ocorrido o retorno da notificação das infrações, estamos enviando as notificações online, pois o mesmo consta registrado no GRAVAME em seu cadastro. Notificações listadas logo abaixo para visualizar basta clicar em cima das mesmas."*

Ao clicar, o usuário é direcionado para o link **http://teachingandlearning.uoit.ca/plugins/content/1pixelout/out.php?Consulta_MultaDERonline**, servidor aparentemente usado para hospedar o código malicioso usado para o golpe digital.

Da análise do cabeçalho do e-mail, podemos identificar que a origem do golpe vem, aparentemente, do IP 201.9.145.28 (provedor de conexão), sendo o provável provedor de serviços responsável pelo e-mail zebu.hnnet.com.br (Itapetininga – Bahia):

Return-Path: <debitos@der.com.br>
X-Original-To: xxxxxxxxxxxxxxxxxxxxx
Delivered-To: xxxxxxxxxxxxxxxxxxxxx
Received: by imap09.uni5.net (Postfix, from userid 1000)

id 62A1C196BBCC; Tue, 18 Jan 2011 19:03:04 -0200 (BRST)
***Received:** from mx2.uni5.net (unknown [10.5.3.92])*
by imap09.uni5.net (Postfix) with ESMTP id 568AE196BB88
for <xxxxxxxxxxxxxxx>; Tue, 18 Jan 2011 19:03:04 -0200 (BRST)
***Received:** from zebu.hnnet.com.br (ns2.hnnet.com.br [201.57.131.67])*
by mx2.uni5.net (Postfix) with ESMTP id 3249D4CB6456
for <jose.milagre@legaltech.com.br>; Tue, 18 Jan 2011 19:03:03 -0200 (BRST)
***Received:** from [10.1.1.2] (201009145028.user.veloxzone.com.br [**201.9.145.28**])*
(authenticated bits=0)
by zebu.hnnet.com.br (8.14.2/8.13.8) with ESMTP id p0IK37nB004826;
Tue, 18 Jan 2011 19:03:20 -0200
*Message-Id: <201101182103.p0IK37nB004826**@zebu.hnnet.com.br**>*
Content-Type: multipart/alternative; boundary=”==========1604917246==”
MIME-Version: 1.0
Subject:
=?utf-8?q?Notifica=C3=A7=C3=A3o_urgente_de_multas_registradas_em_nosso_SI?=
=?utf-8?b?RVIu?=
To: Recipients <debitos@der.com.br>
From: “DER Online” <debitos@der.com.br>
Date: Tue, 18 Jan 2011 19:01:28 -0200

Na montagem do pishing o usuário usa imagens do site oficial do DER e do site de notícias G1. O e-mail foi enviado em massa para diversos usuários. Recomenda-se aos usuários que desejam consultar suas multas que jamais acessem o site do DER por e-mails, short urls ou links, sendo que a consulta pode ser feita diretamente em http://www.der.sp.gov.br/servicos/multas.html por CPF ou RENAVAM.

Para quem recebeu o e-mail, recomenda-se a denúncia em

4dp.dig.deic@policiacivil.sp.gov.br

Igualmente, importante acionar a Polícia Federal em **crime.internet@dpf.gov.br**

Não deixe para lá, denuncie!

CNASI: Painel sobre mobilidade, segurança e privacidade

No dia 19/10/2010 participamos um painel no CNASI – Congresso Latinoamericano de Auditoria de TI, Segurança da Informação e Governança.

Nosso Painel foi sobre "Painel Mobilidade
Mobilidade: privacidade, questões Legais de Segurança". Tive a honra de reencontrar amigos e profissionais como Denny Roger – CEO -EPSEC e Jaime Orts Y Lugo – Presidente ISSA – Information Systems Security Association. O debate abordou questões como uso de internet desprotegida para atos ilícitos, responsabilidade civil e do empregador por atos de seus executivos.

Estimativas revelam que 4 entre 5 executivos do mundo utilizam os dispositivos móveis para negócios. A questão que não cala é: Eles sabem dos riscos? Os equipamentos contram com segurança e criptografia?

Agradeço o IDETI pelo convite à palestrar no evento! O debate foi filmado e em breve disponibilizaremos os links para o download!