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!