Criminosos alteram site do São Paulo FC para infectar internautas

14 de agosto de 2009

Data	Fonte	Crédito da Imagem
14 de agosto de 2009		

Objetivo é instalar cavalo de troia no computador, para roubar dados.
G1 comunicou o problema à Locaweb, do serviço de hospedagem do site.

Um código presente pelo menos desde a noite desta quinta-feira (13) no site oficial do São Paulo Futebol Clube tenta infectar os visitantes da página. Para isso, uma janela do Java pedindo a instalação de um suposto "plug in" é exibida. Se o botão rotulado "Run" for clicado, um cavalo de troia que rouba senhas de banco é instalado. O arquivo malicioso foi identificado como vírus por 10 dos 41 programas antivírus do site VirusTotal.

Clicar em Run neste aviso causa uma infecção no sistema. O vírus roubará senhas de banco. (Foto: JavaPrompt)
O golpe tira proveito de um componente conhecido como Java Web Start. Ele permite que softwares sejam executados no sistema a partir de uma página web. Códigos em Java são normalmente restritos e não podem realizar nenhuma atividade maliciosa, sendo considerados seguros.

Com o Java Web Start, no entanto, é possível "burlar" as permissões normais do Java, mas uma mensagem de confirmação aparece nesses casos. Se o usuário aceitar, o programa será executado com as mesmas permissões que qualquer outro software no PC da vítima. Em outras palavras, clicar em "Run" na janela do Java é o mesmo que baixar e dar dois cliques em um arquivo executável.

A assessoria do São Paulo Futebol Clube não foi encontrada para comentar o caso até a publicação desta reportagem. O G1 também comunicou o problema à Locaweb, prestadora de serviço de hospedagem do site do clube.

Códigos como esse, para infectar os visitantes de sites legítimos, são normalmente inseridos por criminosos virtuais. Eles obtêm acesso ao servidor onde se encontra o site e modificam a página original. Com isso, não se faz necessário o envio de e-mails em massa ou outras mensagens para direcionar internautas a uma página maliciosa. Em vez disso, os próprios visitantes do site atacado tornam-se vítimas.

No final de maio, o site de torpedos da operadora Oi foi alvo de um ataque idêntico.

* Altieres Rohr é especialista em segurança de computadores e, nesta coluna, vai responder dúvidas, explicar conceitos e dar dicas e esclarecimentos sobre antivírus, firewalls, crimes virtuais, proteção de dados e outros. Ele criou e edita o Linha Defensiva, site e fórum de segurança que oferece um serviço gratuito de remoção de pragas digitais, entre outras atividades. Na coluna "Segurança para o PC", o especialista também vai tirar dúvidas deixadas pelos leitores na seção de comentários. Acompanhe também o Twitter da coluna, na página http://twitter.com/g1seguranca.

MARIALVA