

Tira-dúvidas

tecnoguia@diariodonordeste.com.br

MARCOS MONTEIRO

Vírus no pen drive

Agradeço pela excelente ajuda que nos proporciona através de sua coluna. Em sua matéria de 13 de abril de 2009, foi abordada a forma de remover vírus de um pen drive. Eu passei por um teste prático em minha casa, no qual localizei o arquivo "autorun.inf" com o atributo SRH. No entanto, já no prompt do MS-DOS, não consegui excluir o atributo através do comando "attrib -A-S-R-H*". Peço a sua gentileza em detalhar mais o comando a fim de que eu possa fazê-lo. Existe espaço entre os caracteres? Esse asterisco fica mesmo no final do comando? (Adson Bezerra)

Adson, para os sistemas operacionais da Microsoft, você pode dar atributos a um arquivo para que seja um arquivo de sistema, oculto ou somente para leitura. Isso terá como intuito proteger o arquivo de usuários desavisados ou de outros sistemas ou até mesmo de alguns vírus. Os vírus tentam se proteger usando essa mesma técnica e se fazendo passar por arquivos de sistema para impedir a remoção, pois o Windows protege arquivos de sistema, tornando-os ocultos para que os usuários não os vejam e somente para leitura, o que impede sua modificação deste. O comando "attrib" foi feito para manipular arquivos que possuam ou que necessitam de algum atributo. É simples: o comando attrib puro apenas irá exibir todos os arquivos em sua pasta corrente que possuam algum tipo de atributo. Caso você

queira dar um atributo a um arquivo X.TXT, por exemplo, você pode fazer assim: ATTRIB +H X.TXT. Assim, você deu um atributo H (oculto) ao arquivo X.TXT. Ele agora ficará oculto. Outros parâmetros são R (somente leitura) e S (arquivo de sistema). O sinal de "+" é para adicionar o atributo e o sinal de "-" é para remover. Se quiser remover o atributo, então digite: ATTRIB -H X.TXT. Se você quiser adicionar ou remover vários atributos, coloque espaço entre eles: ATTRIB -H +R X.TXT. Se quiser fazer isso em todos os arquivos de uma determinada pasta, basta então usar o "*" para indicar que são todos: ATTRIB -H +R *.

Executei todos os passos para eliminação de vírus do arquivo "autorun.inf" do pen drive, mas ao executar "attrib" novamente o arquivo autorun.inf aparece com todos os atributos. O que posso fazer agora? Formatar o pen drive resolve? (Roberto Campos — Mulungu-CE)

Roberto, o arquivo autorun.inf não é o vírus. É apenas o mecanismo de acionamento do seu vírus. É importante encontrar o programa malicioso que está presente em seu pen drive. É comum que ele esteja na raiz do diretório de seu pendrive com atributos S, R e H. Isso será mostrado assim que for executado o comando "attrib". Então você poderá deletar os arquivos de vírus. É comum também que o vírus se esconda da pasta Recycler, que é a pasta da lixeira. Em seu pen drive esta pasta está escondida. Verifique se você tem essa pasta com o comando "dir /ah" no MS-DOS. Você acessa as pastas através do comando "cd nome da pasta". Dê um attrib, se encontrar nas pastas e subpastas arquivos com esses tipos de atributos é um provável vírus. Os arquivos INFO2 e desktop.ini não são vírus, o resto é provável que seja. Ter um antivírus é sempre importante, pois se seu PC estiver sendo a fonte do vírus, não vai adiantar removê-lo do pen drive, pois será infectado em seguida.

TECNOGUIA

EDITORA VERDES MARES LTDA. - PRAÇA DA IMPRENSA DIONÍSIO TORRES - CEP: 60135.690 - FORTALEZA - CEARÁ - TELEFONES: (085) 3266-9793 - FAX: (085) 3266.9797 - EDITOR: EBENEZER FONTENELE - DIAGRAMADORA: ADRIANA RODRIGUES