



Respostas por Iberê M. Campos e Márcio B. de Carvalho

## MICRO FICOU INFESTADO LOGO DEPOIS DE INSTALAR PROGRAMA ANTIVÍRUS

Uso meu micro principalmente para fazer download de músicas e filmes, por isso o deixo ligado direto. Tenho feito isto há anos, mas acabei me deparando com um problema inusitado. Recentemente fiz a instalação de um programa para remover vírus e trojans, o qual suponho ser da própria Microsoft. O nome do programa é “AV Care” e ele parece realmente ser eficiente, porque logo de cara foi detectando várias ameaças. O problema é que precisa pagar para o programa remover estas pragas, e estou em dúvida se o problema é realmente este. Digo isto porque tenho notado que o micro ficou bem mais lento, e não estou conseguindo navegar com a mesma facilidade de antes. Os sites demoram a abrir ou então simplesmente não abrem mais.

**Cláudio, por e-mail.**

*Esta é uma situação comum, infelizmente. O citado “AV Care”, que se auto-intitula um removedor de vírus, é um grande engodo. Na verdade, o tal de AV Care é um trojan que se veste de “bonzinho” para incitar o usuário a instalá-lo. Este tipo de infecção aparece quando se entra em sites falsos, construídos maliciosamente, com uma janela de fundo fingindo ser da Microsoft, por exemplo, “alertando” para o fato do micro ter sido “infectado” e se oferecendo para fazer a limpeza. Só que esta “limpeza”, de fato, é a própria instalação do trojan que, no caso, é o tal de “AV Care”. Entre outras coisas, o AV Care desabilita o firewall e abre diversas portas de comunicação com a internet que ficam assim à disposição dos hackers, ou seja, o micro fica totalmente exposto à comunidade de malfeitores que povoa a internet.*

*Assim, não causa estranheza alguma o fato do micro ter ficado lento e não conseguir mais navegar. Isto ocorre porque toda a banda de internet disponível para aquele micro passa a ser utilizada para os “serviços” executados pelos trojans e similares, fazendo sabe-se lá o quê. Com certeza, não deve ser nada do bem.*

*A técnica de remoção de vírus que detalhamos na Revista PnP nº 2 é bastante eficaz nestes casos. Também existem ferramentas para remover programas específicos, como o citado AV Care. Fora isto, uma providência simples que pode ser tentada é esta:*

- 1 *Desligue a “Restauração automática do sistema”.*  
*Para tanto, vá nas “Propriedades” do “Meu computador” e depois na aba “Restauração do sistema”.*
- 2 *Instale um BOM antivírus, devidamente atualizado*
- 3 *Entre no modo de segurança do Windows e faça uma varredura completa no micro, removendo todos os arquivos infectados que forem encontrados.*
- 4 *Reinicialize em modo normal e use um programa de limpeza de registro como o Ccleaner ou o Norton WinDoctor, apagando todas as entradas inválidas.*
- 5 *Reative a “Restauração automática do sistema”.*

*Com isto o micro deve retornar ao funcionamento normal, a não ser que o malware tenha feito estragos na instalação do Windows. Em especial, alguns worms modificam a parte de rede e de internet, e estes reparos podem ser difíceis de serem feitos. Se a instalação ficou muito danificada, a melhor solução costuma ser a mais radical: copiar os dados do usuário, formatar o HD e fazer uma nova instalação a partir do zero, conforme aconteceu no caso a seguir:*

### DICA

Para conhecer mais sobre vírus e as técnicas que usamos para detectar e removê-los, recomendamos a leitura dos dois artigos sobre este assunto publicados na Revista PnP nº 2 (vide capa ao lado).



## NOTEBOOK PEGOU VÍRUS E AGORA NÃO NAVEGA NA INTERNET

Sou técnico em informática e estou apanhando para consertar o notebook de um cliente. Ele deve ter aberto um email que continha algo que desativou o antivírus e também o firewall, abrindo as portas para centenas de worms e