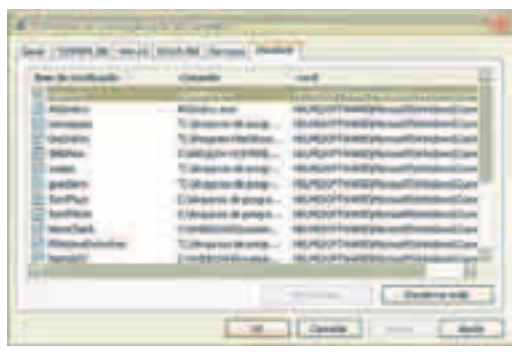
CONTINUAÇÃO DA CAPA

SE VOCÊ COMPROU ANTIVÍRUS FALSIFICADO, SAIBA COMO FAZER PARA ELIMINAR AS PRAGAS VIRTUAIS DO COMPUTADOR

COLOQUE O "CAVALO" PARA CORRER

PARA REMOVER O TROJAN

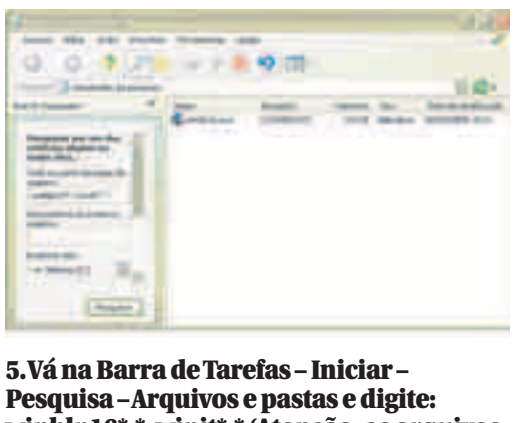
1. Na Barra de Tarefa – Selecione Iniciar – Executar e digite "msconfig" – sem aspas e tecle OK.



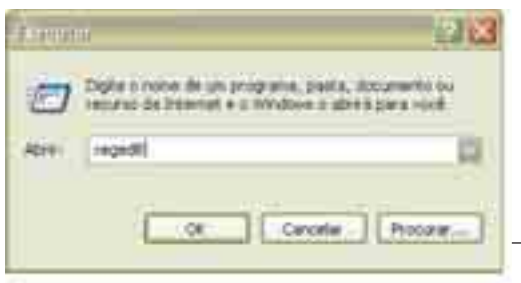
2. Na aba Inicializar desmarque os quadradinhos relacionados com os arquivos: winhlp16.exe e winit.exe.

3. Reinicie a máquina.

4. Abra o Windows Explorer e na Barra de Menu, selecione Ferramentas – Opções de pasta. Na aba Modo de exibição e em Configurações avançadas desmarque a opção [ ] Ocultar arquivos protegidos do sistema operacional e marque a opção [x] Mostrar pastas e arquivos ocultos.

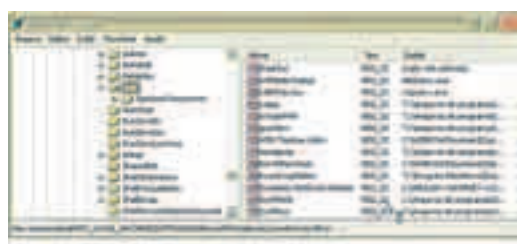


5. Vá na Barra de Tarefas – Iniciar – Pesquisa – Arquivos e pastas e digite: winhlp16*.*; winit*.* (Atenção: os arquivos são separados por ";", ponto e vírgula). Após apagar os arquivos, remova-os da Lixeira, também.

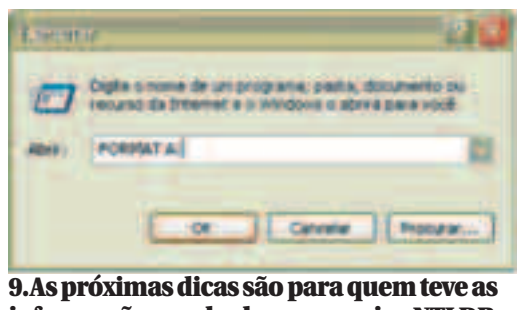


6. Vá em Iniciar – Executar e digite "regedit" sem aspas.

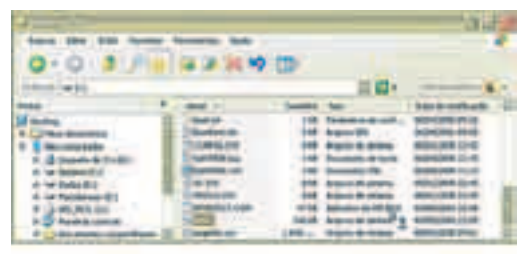
7. Será aberta uma janela com o Editor do Registro. Você deve ir clicando no sinal de "+" para expandir as chaves do Registro começando por HKEY_LOCAL_MACHINE\SOFTWARE...



8. ...Até chegar na chave final: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run Apague, na janela da direita, todas as referências aos arquivos "winhlp16.exe" e "winit.exe".



9. As próximas dicas são para quem teve as informações roubadas e o arquivo NTLDR apagado: No Menu Iniciar selecione Executar, insira um disquete na unidade e digite "format A:"



10. Agora vá num micro que tenha a mesma versão do XP de sua máquina, acesse o disco C e copie os seguintes arquivos: boot.ini, NTLDR e ntdetect.com. Carregue o sistema operacional pelo disquete, dê login na máquina e copie para o disco C o arquivo NTLDR.

Pescaria na internet

O golpe aplicado nos usuários do pacote de soluções falsificado do Norton não é novidade. De acordo com o *Anti-PhishingWorking Group* (APWG), somente em fevereiro deste ano foram informadas 13,2 mil novas mensagens fraudulentas, um aumento de 2% em relação a janeiro deste ano e de 26% se comparado a julho de 2004. O grupo registrou ainda que 64 marcas comerciais foram usadas pelos cibercriminosos.

Você certamente já deve ter ouvido falar em *Phishing Scam*, mas pode não saber exatamente o mal que ele pode causar. *Phishing* vem do termo em inglês pescar e é o nome dado à técnica de enganar internautas com falsas mensagens eletrônicas enviadas em massa. Os e-mails são muito parecidos com os verdadeiros: têm logotipo da empresa, endereços de email e links. Ao clicar no link o internauta morde a "isca". No lugar de remeter o internauta ao site da instituição prometida, ele leva a um outro idêntico. Quando a conta e a senha, por exemplo, são digitadas começa o golpe. Assim como contas bancárias, qualquer outro dado pessoal pode ser coletado. Número do cartão de crédito, CPF, identidade, endereço, entre outros.

O APWG estima que 5% das pessoas que recebem os spams caem na armadilha. A consultoria de segurança britânica mi2g garante que este tipo de golpe cresceu 330% entre 2003 e 2004. E como se não bastasse, a forma de "abordagem" dos criminosos está mudando. O APWG detectou que já é bastante presente na internet a "pescaria sem isca". As técnicas mais usadas são a *Pharming*, a *keylogging* e a contaminação do DNS.

Uma das mais registradas é quando o código malicioso modifica o arquivo host e informa ao site falso as páginas mais acessadas por um certo usuário. Essa prática é chamada de *Pharming*. O *keylogging* acontece quando o código trava as teclas do micro e registra os caracteres digitados para acessar um grupo de URLs pré-determinado, como os de instituições financeiras. A contaminação do cache do DNS é usada para transmitir informações para websites ilegais de *pharming*.

O Websense Security Labs garante que um número elevado de pequenos sites de e-commerce e de bancos regionais estão sendo vítimas do *phishing*. De acordo com o último relatório do APWG, o Brasil já é o quarto colocado no mundo em ataques desse tipo e fica atrás apenas dos Estados Unidos, do conjunto China-Taiwan-Hong Kong e da Koreia. Depois do Brasil vêm Alemanha, Japão, Canadá, Argentina e França. Portanto, todo cuidado é pouco. (**Marina Amazonas**)

LUIZ HENRIQUE QUEMEL
ESPECIAL PARA O **CORREIO**

Se a cópia pirata "geneticamente" modificada foi instalada em seu PC, você deve seguir alguns passos (*leia quadro*) para inabilitar os códigos maliciosos e mandar o cavalo de tróia pastar em outra freguesia. Mas é bom saber que a máquina pode ficar com seqüelas. O ideal é que a unidade seja completamente formatada, com a instalação depois do antivírus e do firewall originais.

O filósofo grego Heráclito já dizia que nenhum homem se banhava no mesmo rio por duas vezes. Na segunda vez, nem o rio nem o homem eram os mesmos. Partindo desse princípio teríamos a Lei Universal de Segurança que diz: "(...) se alguém mal intencionado puder executar programas, modificar o sistema operacional ou ter acesso físico a seu computador, este não mais lhe pertencerá". Embora as instruções removam o trojan, Heráclito nos sugere com sua filosofia que nosso PC nunca mais será confiável após um ataque desses. Por isso, aconselho a todos os usuários que adquiriram e instalaram o programa pirata a formatar completamente o micro, começando tudo de novo. Dessa vez, com o antivírus e firewall originais.

Para quem teve informações roubadas e o arquivo NTLDR apagado, o ideal é mudar urgentemente todas as senhas — caso você tenha acessado páginas de bancos. Depois, para restaurar o arquivo NTLDR, vá em outra máquina com o Windows XP instalado, formate um disquete e copie os seguintes arquivos para ele: NTDETECT.com, boot.ini e o próprio NTLDR.

A carga do sistema será feita pelo disquete. Após efetuar o login na máquina infectada, copie o arquivo NTLDR.exe para o disco rígido (normalmente o C:). Nesse momento e numa fração de segundos surgirá uma janela do DOS tentando apagar novamente o arquivo. Como ele está no disquete, ocorrerá um erro. Após esse evento siga os passos descritos no quadro a partir do primeiro e sua máquina estará livre do cavalo de tróia.