Sobre o vírus

Há um vírus, “Shortcut link virus”, que oculta as pastas de um pendrive e cria um script que executa a infecção do vírus para o computador e, em seguida, abre um atalho para essas pastas ocultadas. Ele é caracterizado como um Worm Autorun. Quando infecta um PC, somente Windows, este vírus cria pastas com nomes codificados, aleatórios e dinâmicos, como 7020, 96ce, jc3, etc., contendo arquivos de java script, extensão .js, os quais estão programados para interferir no comportamento do computador e infectar novos pendrives.

Removendo o vírus do pendrive

Para os seguintes comandos, cada linha é um comando diferente.

Linux:

Digite os seguintes comandos em um terminal (tecle Alt+F2 e digite xterm ou gnome-terminal e clique em Executar):

1. `mkdir /mnt/pendrive`
2. `mount /dev/sdb /mnt/pendrive`
3. `rm -rf *.lnk`
4. `rm -rf pastascomvirus`
5. `rm -rf autorun.inf`
6. `find . -exec sudo fatattr -h '{}' \;`

Windows:

Digite os seguintes comandos em um prompt de comando (tecle *Windows+R*, digite *cmd* e tecle *Enter* ou vá em Menu Iniciar→Todos os Programas→Acessórios→Prompt de Comando):

1. `X:`
2. `del /f /s *.lnk`
3. `del /f /s autorun.inf`
4. `rmdir /s /q autorun.inf`
5. `attrib -h -s -r /s /d X:\*.*`
6. `del /f /s pastascomvirus`
7. `rmdir /s /q pastascomvirus`

Obs: Assumindo que o pendrive seja o dispositivo sdb e pastascomvirus sejam as pastas que possuem o nome aleatório e contenham, ou os java scripts, ou nada dentro:

Removendo o vírus do computador

Windows 7:

1. Reiniciar o computador e apertar repetidamente e freneticamente a tecla F8 (Entrar em Modo de Segurança)
2. Verifique se existe um arquivo JScript (extensão .js) em Menu Iniciar→Todos os Programas→Inicializar.
3. Abra a pasta Inicializar (Caminho inteiro da pasta oculta: C:\Users\usuário_infectado\AppData\Roaming\Microsoft\Windows\Start Menu\Startup)
4. Exclua o arquivo .js e feche a pasta.
5. Faça o comando Windows+R (Executar no Menu Iniciar)
6. Digite msconfig
7. Vá para a aba Inicialização de Programas e desmarque a entrada do .js
8. Reincie normalmente.

Windows XP:

1. Reiniciar o computador e apertar repetidamente e freneticamente a tecla F8 (Entrar em Modo de Segurança)
2. Verifique se existe um arquivo JScript (extensão .js) em Menu Iniciar→Todos os Programas→Inicializar.
3. Abra a pasta Inicializar (Caminho inteiro da pasta oculta: C:\Documents and Settings\usuário_infectado\Dados de Aplicativos\Microsoft\Windows\Menu Iniciar\Inicializar)
4. Exclua o arquivo .js e feche a pasta.
5. Faça o comando Windows+R (Executar no Menu Iniciar)
6. Digite msconfig
7. Vá para a aba Inicialização de Programas e desmarque a entrada do .js
8. Reincie normalmente.

Aplicar uma vacina no pendrive

1. Abra o diretório raíz do seu pendrive.
2. Crie uma pasta chamada **autorun.inf** ou/e **autorun.ini**
3. Abra essa(s) pasta(s) e crie outra pasta com o nome **a**
4. Pronto. Seu pendrive já está protegido!

Obs: Alguns testes desta vacina não foram bem sucedidas, devido às novas formas mais inteligentes do vírus. No entanto, este método irá prevenir seu pendrive contra ataques de outros Worm Autorun também.