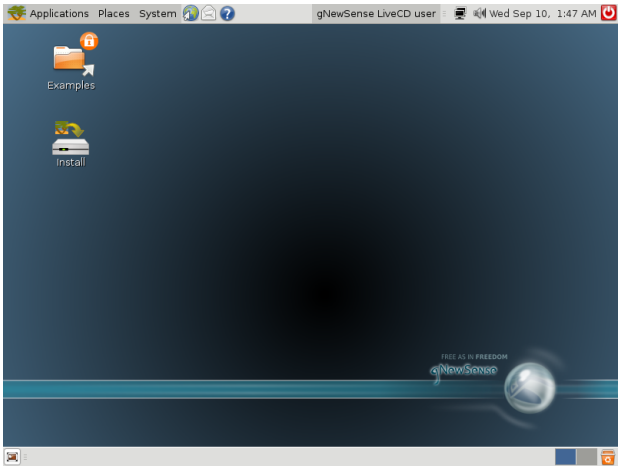
Vírus no Linux?

Este artigo abaixo foi produzido originalmente para a Network Core Wiki. Reproduzo-a aqui na íntegra. Publicado originalmente em 07/12/2007.



Interface de uma distribuição Linux

Uma das grandes perguntas dos iniciantes, no uso de sistemas operacionais Linux, é se estes sofrem a ação dos vírus de computador.

Para responder essa questão devemos analisar alguns pontos importantes.

Vírus de Computador

O que seria bem um vírus de computador?
Numa consideração "lato sensu", ou seja, ampla, qualquer programa com função maliciosa é um vírus. Entretanto, numa visão mais técnica e "strictu sensu", os vírus são programas maliciosos que têm técnicas de reprodução, explorando falhas nos sistemas, de forma que possam se replicar para outros computadores.

Assim, um vírus que se envia por e-mail para toda a sua lista de endereços, ou aquele que se replica no pen-drive etc, são programas que exploram falhas no sistema e procuram se

replicar de um computador para o outro, além de efetuarem os estragos a que estão programados.

[meuadsense]

Um cavalo de Tróia, no modo estrito de responder o que é um vírus, pode não ser considerado, em última instância, como um vírus que se auto-replica (pois estes nem sempre têm mecanismo de reprodução, por vezes são apenas iscas para garantir invasões de intrusos em sua máquina): há aqui o efeito psicológico envolvido – o usuário, que é humano, pode ser ludibriado psicologicamente a executar tais códigos de forma que estes possam permitir danos por crackers invasores.

Entretanto, se pensarmos da forma ”lato sensu”, podemos considerar vários tipos de códigos maliciosos como vírus; mas para este intento deveríamos ter um leque enorme de tipos de vírus de computador.

O funcionamento do Windows

Em geral no Microsoft Windows (principalmente 3.x e 9.x) não há uma estrutura de permissões bem construída a respeito de cada arquivo, do sistema ou não.
Isso significa que no Windows 98 se, por exemplo (e ainda, infelizmente, nos mais atuais também) eu executar um arquivo com código malicioso este, por sua vez, pode alterar arquivos do sistema, pois eu tenho, a possibilidade de alterar diversos arquivos do sistema.
Apesar das versões mais recentes do Windows tentarem bloquear certos arquivos, esta política não é tão bem estruturada (na verdade não é um trabalho de escalonar permissões legítimas).
A forma do funcionamento do Linux é toda voltada para usuários. Cada usuário pode ter diversas permissões para se trabalhar com os arquivos do sistema (em geral apenas o Super Usuário, ou administrador, tem a possibilidade de apagar certos arquivos do sistema). Assim para executar um vírus “letal” no Linux, eu o teria de executar como super usuário.

Outra coisa importante é a diferença entre EXECUTAR e ABRIR algum arquivo. No Windows essas nomenclaturas se confundem. No Linux isso é bem definido: executar é diferente de abrir um arquivo, e para executá-lo devemos atribuir permissão de execução.

Um código malicioso sem a permissão de apagar arquivos do sistema só poderia apagar arquivos do usuário (o que de uma certa forma reduz o poder de destruição). Para evitar essa destruição, basta saber o que se está executando.

O Sudo

Mas no linux existe um software chamado ”sudo”, que permite com que eu executa um comando de super usuário com a senha do usuário comum. Aqui, alguns dizem, pode residir a possibilidade de se executar um código malicioso (ou, se formos a modo ”lato sensu”, vírus).
Entretanto, mesmo assim um suposto vírus deveria estar com permissão de execução, e o usuário, na maioria das vezes, deveria que inserir sua senha para que este código efetuasse seu estrago.

Fator externo

Para um código de cunho malicioso efetuar algum estrago relevante no linux então ele deve explorar falhar muito sérias no sistema (que por ser código aberto poderiam ser corrigidos) e algumas artimanhas que poderiam beirar a manobras psicológicas (como oferecer algo em troca se for executado um script, etc). Apesar disto as alternativas de um vírus estão reduzidas, devido a estrutura do software, mas não impossível de que se crie um código malicioso.

É possível?

Sim, é possível que exista códigos maliciosos, mas estes tem o escopo de ação reduzido e não tão grande como os que encontramos nos milhares e milhares existentes para o Windows.

Apesar de tecnicamente ser possível, não há registro de vírus “potentes” que tenham efetuado estragos enormes em sistemas linux.

Com toda essa estrutura do sistema linux, basta se ter cuidado para não executar códigos maliciosos que porventura venham a existir.

[meuadsense]

Antivírus no Linux

Existem sim antivírus para Linux, mas a principal função destes é na aplicação de servidores (como servidores de e-mail etc) que se comunicam com máquinas Windows.
Levando em consideração que um vírus projetado para Windows não atacaria necessariamente o Linux (a exceção ocorreria, em possibilidade, com o módulo Wine, mas se isto acontecesse tecnicamente apenas uma pasta seria destruída).
Pois bem, como os vírus ”for Windows” não atacam necessariamente um linux, um servidor Linux poderia nada sofrer apesar de poder se tornar um meio de propagação indireta do vírus numa rede. Assim os antivírus no linux servem, em última instância para procurar vírus de Windows e apagá-los (e não propagarem indiretamente estes códigos).

A questão usuários x arquitetura do software

Levando em consideração a arquitetura do software sistema operacional (como foi exposto a respeito das permissões de arquivos) podemos levar em consideração que este é um dos fatores a respeito da proliferação de vírus em um dado sistema operacional.

Outro fator na grande quantidade de vírus para Windows (além das falhas que estes exploram) é a sua popularidade (mas vale lembrar que a ”’questão da popularidade não responde todas as perguntas”’).
Existem mais códigos maliciosos no Windows porque este é mais

popular. E eles ainda fazem muito estrago, pois a produção do Windows é centralizada; ou seja a correção em falhas no sistema depende de uma única empresa: E estas falhas ainda existem.

A quantidade de usuários de um sistema é um fator na quantidade de vírus produzidos para aquele, ou outro sistema, mas esta é somente a ponta do iceberg. ”’O principal fator está ligado às falhas no software”’, ou seja ”’o fato de existir mais usuários Windows não é o fator preponderante na existências de vírus para este sistema, mas sim suas falhas consideráveis”’.

Vírus ”for Windows’‘

De uma certa forma, tais vírus criados para Windows são praticamente ineficazes no linux. Por isso a enorme gama de vírus para Windows não teriam eficácia alguma no Linux.
Apesar disto deve-se ter alguns cuidados básicos, como não executar scripts desconhecidos como super usuário. ”’Deve-se evitar de usar o super usuário como um usuário padrão”’.

[meuuol]

Apesar de praticamente improvável de acontecer certos estragos como se conhece no sistema Windows, deve-se obedecer certos cuidados para evitar até mesmo os pequenos males. Pois se os grandes já são evitáveis, é interessante ter consciência para se não executar aqueles cuja dor de cabeça é menor – mas por que si já seriam dor.

Arnaldo Vasconcellos