

# Existem vírus para Linux?

Author: André Felipe Machado<clubes@techforce.com.br>

Sim, 666 mais recente é de 2005.

A Trend Micro 5,5 milhões de vírus e ameaças para MS-Windows.

E que a indústria de antivírus mentiu por 20 anos dizendo que conseguia proteger os usuários.

Os tais vírus para Linux só conseguiram contaminar máquinas que não tinham sido atualizadas para correção de segurança. Os administradores esquecidinhos ou atrasadinhos....

Neste artigo de ver estas informações.

E olha que nesses 863 englobam toda ameaça automatizada contra o Linux, como root kits, worms e scripts para invasão.

Um conceito muito mais abrangente do que usado na definição para windows\*.

Este artigo foi escrito originalmente em junho de 2005. Em janeiro de 2008, um outro autor voltou ao tema, corroborando, revalidando e agregando novas informações.

Em julho de 2008, outro autor estudou

Mas se windows\* já tem mais de 360 MIL vírus e ameaças de todo tipo, e todo dia surgem mais, por que tão poucos no Linux?

Alguns fatores combinados.

Você pode ler um pouco mais [aqui](#) [aqui](#)

- Engenharia social
- Arquitetura do sistema
- Configurações do sistema
- Comunidade de desenvolvedores e usuários
- Modo de usar do sistema.

## Engenharia social

A maioria dos spam e sites virulentos usa velhos truques para ATRAIR os usuários a fazer alguma coisa, como ler email (só ler já pode contaminar no windows\*), abrir um anexo, visitar um site (sim, você pode contaminar a máquina enquanto fica babando por aquela foto gostosona num site).

Apelam para instintos básicos, como medo (será que levanta agora?), insegurança (será que é pequeno?), luxúria (gostooosa!), ganância (fique rico sem fazer nada), etc.

## Arquitetura do sistema

No Linux, Unix e outros, o projeto é diferente. Se levou segurança em consideração desde a idealização, conceito inicial. Assim, é muito mais difícil inventar vírus para eles. E quando se consegue, espalham-se muito menos, pelos outros fatores.

[Não existe](#) sistema inexpugnável.

## Configurações do sistema

No [Debian GNU / Linux](#) FreeBSD, no Unix, e em um grau um pouco menor nas outras grandes distribuições linux, as configurações default seguem um conceito básico:

**Tudo** está fechado,  
**nada** é permitido até que o administrador autorize.

Quanto mais aberto e mais permitido ficam as configurações, mais "fácil" é a distribuição.

Chega ao extremo do Kurumin, derivado do Knoppix, e Linspire que são configurados com quase tudo liberado totalmente, o que os torna quase tão "fáceis" e inseguros quanto windows\*.

Adianta comprar um cofre e colar na porta um Post-It\* com a combinação?

Aliado a configurações default mais seguras, dificilmente os sistemas são configurados exatamente iguais.

## Comunidade de desenvolvedores e usuários

Um dos sustentáculos do Linux é uma comunidade forte.

E o Debian ~~participa das~~ [participa das](#) [mais fortes](#) [comunidades de desenvolvedores e usuários](#). ~~Sim,~~ usuário informado é valioso.

A rápida troca de informações viabiliza reações e soluções rápidas, minimizando danos.

Existe uma [equipe formal de segurança](#)

[Bug reports](#) são levados muito a sério, rapidamente e às claras.

## Modo de usar o sistema

O Linux implementa totalmente o conceito de usuário e permissões e deve ser usado assim.

Um usuário pode fazer determinadas coisas, usar determinados programas, ter acesso a determinados arquivos.

Até mesmo os programas funcionam dentro de um ambiente de usuário.

Isso torna mais "difícil" a configuração (precisa autorizar explicitamente) e o "uso" (se não foi autorizado, não pode).

Algumas distribuições, com já citado, deturpam esse conceito, para "facilitar", mas aumentando o risco de segurança demais.

No modo correto de uso, fica intrinsecamente limitado o tipo e a extensão de danos que um vírus ou invasor pode causar.

Esse conjunto de fatores também leva ao fato de que a quase totalidade dos ataques a máquinas linux seja MANUAL.

O atacante normalmente usa algumas ferramentas para examinar a máquina, tentando descobrir que portas estão abertas, e quais programas e versões estão operando. Procura principalmente versões desatualizadas e ou inseguras.

Aí geralmente ele cruza dados numa matriz de ataque, e decide que ferramentas usar e envia comandos e ou scripts e verifica que tipo de benefícios ele poderá ter.

Embora seja mais complexo que isso, você já notou que é uma situação diferente, com soluções diferentes também.

## Usuários comuns estão em perigo?

Ao ~~levar a configuração~~ precisa ser autorizado de como os usuários são parte importante do problemão que se tornaram os vírus no windows\*.

E horrorizado de como o fabricante aborda o problema.

Inevitavelmente,  
~~sempre o usuário~~ sempre o usuário ficará com o prejuízo custos

Um ditado corrente entre os administradores de informática é de que não há nada mais perigoso que um usuário inocente e ingênuo.

Por isso [seque distribuições linux mais preocupadas com segurança, como o Debian](#) preocupam em configurar e funcionar protegendo o usuário dele mesmo.

Pode até ficar um pouco mais "difícil" ou trabalhoso no início, para autorizar explicitamente o que você quer fazer.

Mas os ganhos ao longo prazo são plenamente compensadores.

## Para usuários muito assustados com segurança tem solução?

Se bancos e até os computadores do Pentágono já foram invadidos, o que se pode fazer?

Para os realmente apavorados com segurança, ou que têm dados extremamente sensíveis, podem analisar o [Debian com as modificações Linux \(Security Enhanced Linux\)](#) criada pela NSA (National Security Agency).

**Esses** são paranóicos com segurança.

Veja na página citada PORQUE escolheram Linux.

## Por que, então, existem programas antivírus para Linux?

O Linux é muito usado como servidor de arquivos, de impressão, de email, firewall, proxy, web, intranet, internet, extranet, e até de aplicação (1) para redes de clientes windows\*.

Assim, muitos arquivos e tráfego windows\* passam por dentro dele.

Portanto, é um bom local para instalar um programa antivírus para limpar arquivos e tráfego, para proteger a si e aos clientes windows\*.

(1) é possível instalar windows\* DENTRO do Linux, encapsulando-o dentro de um ambiente mais seguro. Há alternativas desde integração quase completa até isolamento completo

(máquinas virtuais). Mas ainda é windows\*, um pouco mais seguro e com algumas vantagens de recuperação, mas não é linux.

(2) O ~~projeto Debian~~ [projeto Debian](#) adiciona SELinux como default na futura versão estável. Atualização 22 jan 2008: SELinux está disponível no Debian 4.0 lançado em abril de 2007.