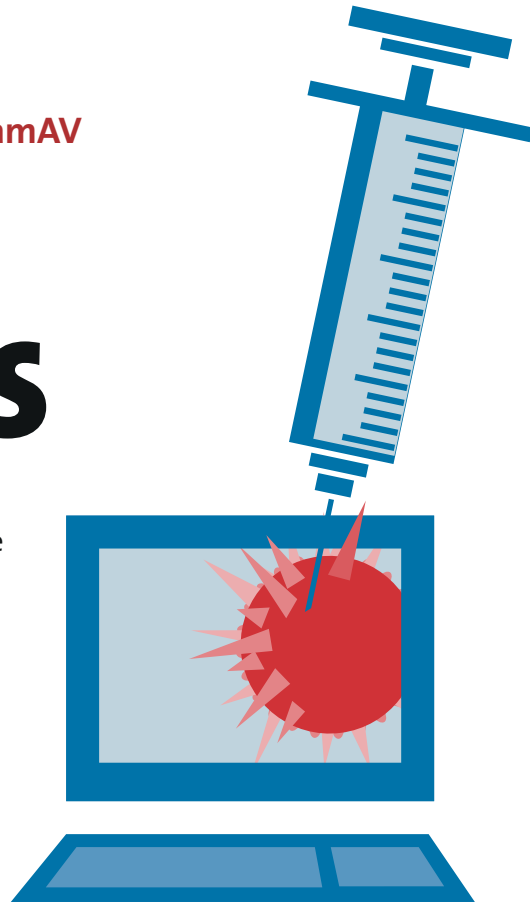


**Combatendo vírus do Windows no Linux: ClamAV**

# Mariscos medicinais

Os programas maliciosos, atualmente, estão mais fortes do que nunca. Embora isso afete pouco um sistema Linux no estado da arte, quem usa tanto Windows quanto Linux pode sem dúvida beneficiar-se de um filtro antivírus. **POR MARC ANDRÉ SELIG**



**V**ocê provavelmente já ouviu alguém dizer: “A melhor forma de proteger um computador é cortar os fios.” Admitamos que essa piada já está um tanto ultrapassada. Na era das baterias de alto desempenho e das redes sem fio, a remoção da energia e dos cabos de rede pode não bastar para impedir a entrada de intrusos (veja o quadro 1).

O exemplo da pág. 23 mostra como você pode se proteger contra atacantes humanos. Firewalls, atualizações de sistema constantes ou uso moderado de serviços de rede podem ajudar. Neste artigo, analisaremos um “malware” automatizado, que pode atacar suas máquinas sem nenhuma ajuda humana.

Há três categorias principais: vírus genuínos em geral afetam os arquivos executáveis de um computador e em compartilhamentos de rede. São acionados sempre que se abre um programa infectado. Já os trojans dependem mais ou menos de um usuário que os copie para sua máquina e os abra. Os Worms vão além e propagam-se entrando automaticamente em serviços vulneráveis ou enviando-se por email para novos alvos.

Uma distribuição Linux com todas as atualizações (patches) aplicadas deveria ser praticamente imune a esse tipo de praga. Os Vírus, no sentido próprio da palavra, já têm bastante trabalho para atacar sistemas Unix. Um usuário não-privilegiado que utilize um programa normalmente não tem permissão para modificá-lo. Worms e Trojans são mais cheios de truques. Felizmente, o Linux (ainda) é visto como um alvo pouco atraente pelos crackers que constroem os worms. Além disso, as vulnerabilidades encontradas nos programas de código aberto em geral são corrigidas em poucas horas. Portanto, não há razão para se preocupar, se seu sistema estiver atualizado.

As coisas não são tão simples se você usar o Windows junto com o Linux. As vulnerabilidades nos programas da Microsoft com frequência permanecem sem correção por meses – buracos escancarados que oferecem vetores de ataque de uso fácil. Não importa se você tem uma instalação do Windows paralela em seu computador ou computadores diferentes com Windows em sua rede doméstica, o Linux pode ajudá-lo a proteger essas outras máquinas.

Neste artigo conheceremos um antivírus para Linux que analisa automaticamente as mensagens que chegam ou os compartilhamentos Windows acessíveis ao Linux.

## Antivírus Grátis

Há um certo número de antivírus disponíveis para Linux, assim como para Windows. Alguns são gratuitos, outros comerciais [4,5]. A maioria deles é projetada para eliminar vírus e worms. Afinal de contas, os usuários de Linux geralmente preferem consertar as vulnerabilidades, em vez de perseguir worms o dia inteiro.

Mais especificamente, discutiremos o ClamAV [1], um genuíno produto Open Source, neste artigo. Se você precisa de uma proteção mais completa, pode preferir usar um segundo programa, mas as técnicas que analisaremos são genéricas e aplicam-se da mesma maneira a quaisquer programas que você possa escolher.

A caça aos vírus completamente automatizada não é exceção à regra “quem não chora não mama”. O mais desagradável na instalação é o fato de que o ClamAV necessita de uma biblioteca

## Listagem 1: Instalando o ClamAV e o Clamassassin.

```

01 $ su
02 Password: root-password
03 # groupadd clamav
04 # useradd -g clamav -s /bin/z
    false clamav
05 # exit
06 $ tar xzf clamav-0.70-rc.tar.z
    gz
07 $ cd clamav-0.70-rc
08 $ ./configure --sysconfdir=
    /etc
09 [...]
10 $ make
11 [...]
12 $ su
13 Password: root-password
14 # make install
15 [...]
16 # exit
17 $ cd ..
18 $ tar xzf clamassassin-
    1.0.0.tar.gz
19 $ cd clamassassin-1.0.0
20 $ su
21 Password: root-password
22 # install clamassassin /usr
    /local/bin
23 # cd /usr/local/bin
24 # ln -s `which mktemp` .
25 # ln -s `which formail` .
26 # exit
27 $

```

## Portas dos Fundos

Quais vetores de intrusão um atacante poderia utilizar para comprometer sua máquina? O método mais óbvio é o uso de um serviço de rede para acessar seu sistema. Muitos sistemas Unix rodam um servidor Web, como o Apache. Se esse servidor tiver uma vulnerabilidade, um cracker malicioso pode conseguir atacá-lo abrindo uma conexão com o servidor Web e transferindo um **exploit**. Em uma máquina particular, você pode se proteger contra esse vetor de ataque desabilitando serviços ou mesmo deixando de instalá-los.

Em princípio, todos os dados externos contêm um exploit. Após baixar uma mensagem de email em sua máquina, o simples ato de abri-la pode permitir que um atacante explore uma vulnerabilidade. O Outlook e o Outlook Express, em particular, são famosos por sofrer de vulnerabilidades desse tipo. É isso que torna filtros antivírus para email tão importantes.

Navegadores web também podem ser vulneráveis, oferecendo um vetor de ataques quando usados para visualizar um website externo. Alguns desses problemas podem ser resolvidos com a utilização de um **proxy**, outros não.

Até recentemente, vírus e worms eram tipicamente propagados por meio de sistemas de arquivos de rede, como por exemplo compartilhamentos Windows com acesso livre. Esse problema foi mitigado em grande parte com opções de uso do Windows mais restritivas e o aumento do uso de filtros de pacote.

Alguns vetores de acesso são bastante enigmáticos e os usuários domésticos têm poucos meios de se proteger contra eles. Quase todos os protocolos básicos podem ser explorados se o programa rodado neles for vulnerável. A História registra uma porção de contos sobre worms que exploram o **DNS** ou algum protocolo **ICMP**.

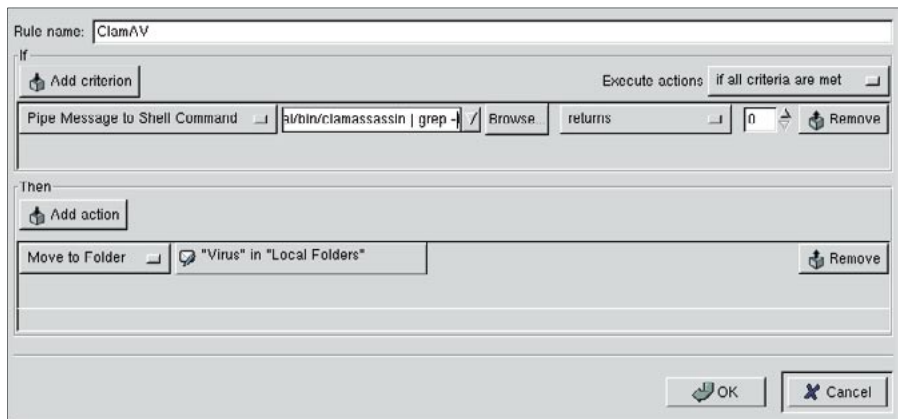


Figure 1: Uso do ClamAV com o Evolution.

chamada MP [2], que a maioria das distribuições não instala. Confira antes de tudo os arquivos de sua distribuição para ver se você tem a biblioteca, e só depois tente instalar o ClamAV!

A instalação do ClamAV em si é bastante parecida com a instalação Linux típica. O manual traz as diretrizes sobre a instalação do programa a partir do código fonte. A Listagem 1 traz uma visão geral do procedimento. Se você está utilizando um sistema *stand-alone*, é bom acrescentar o utilitário *clamassassin* [3]. Ele permite conectar o antivírus a seu sistema de email sem que seja necessário reconfigurar seu **servidor SMTP**. Isso é mais simples, mas também menos eficiente do que as outras soluções. Preste atenção às crases nos comandos “*ln -s*”.

Você pode testar o ClamAV imediatamente após terminar a instalação. Por exemplo, se a sua partição Windows estiver montada em */windows*, o comando de verificação será o seguinte:

```
clamscan -ri /windows
```

## Procurando por vírus

O que torna o ClamAV realmente interessante é sua capacidade de verificar automaticamente as mensagens de email que chegam. A forma como você o conecta a seu sistema de email favorito é mais ou menos uma questão de gosto.

Muitos usuários configuram um verdadeiro servidor de email em sua máquina Linux local. O utilitário Suse YaST, por exemplo, permite fazê-lo. Uma pequena ferramenta chamada *fetchmail* recolhe as mensagens que chegam no servidor de seu provedor e as envia a seu próprio servidor de email. Por isso, seu servidor de email guarda as mensagens em */var/mail* ou */var/spool/mail*. Essa variação aumenta ainda mais a eficiência dos softwares de email populares.

O modo mais fácil de adicionar o ClamAV a um sistema *stand-alone* configurado dessa maneira é com o **procmail**. Para fazê-lo, simplesmente acrescente a Listagem 2 no início de seu *~/procmailrc*. Se esse arquivo não existir em seu diretório padrão do usuário (*/home/usuario*), basta criá-lo.

Quem prefere uma opção mais confortável e utiliza um cliente em GUI como o Evolution ou o Kmail para receber suas mensagens diretamente a partir do servidor não tem que ficar sem o ClamAV. Claro, é preciso decidir se um filtro antivírus realmente é necessário

## GLOSSÁRIO

**SMTP:** O serviço responsável pelo envio (e, em provedores de internet, recebimento) de mensagens de email. Normalmente roda como um processo em segundo plano. SMTP é a abreviatura de "Simple Mail Transfer Protocol" [Protocolo Simples para Transferência de Email], a "linguagem" utilizada pelos servidores de email para trocar mensagens.

**groupadd:** Comando que cria um novo grupo de usuários, "clamav", na Listagem 1. Talvez você precise digitar o caminho completo, "/usr/sbin/groupadd" para rodar o programa.

**useradd:** Comando que permite ao usuário "root" adicionar uma nova conta de usuário ao sistema. Use o flag -g para especificar o grupo e -s para especificar o shell de login para o usuário. Na Listagem , "/bin/false" garante que ninguém será capaz de se logar com a conta do usuário clamav. Esta conta só é necessária para rodar programas.

**install:** O programa "/usr/bin/install" copia a ferramenta clamassassin para o diretório "/usr/local/bin".

**procmail:** Este poderoso MDA (agente de entrega de emails) recebe as mensagens que

chegam e as armazena em um arquivo em disco. Há diversas variações de configuração, como separar as mensagens segundo diferentes critérios. A maioria das distribuições Linux modernas habilitam o procmail por padrão quando um usuário cria um arquivo ~/.procmailrc. Se no seu sistema for diferente, visite [6] para mais informações.

**Pipe:** O caractere pipe | usa a informação (saída) dada pelo comando à sua esquerda como entrada de dados no processamento do comando à sua direita.

**Cron:** Este daemon roda em segundo plano e inicia programas automaticamente em momentos específicos. Isso inclui a busca por nova documentação uma vez por dia ou o arquivamento dos arquivos de log do seu servidor web uma vez por mês. As chamadas "crontabs" (abreviatura de "cron tables") contêm listas de tarefas agendadas, organizadas segundo as contas de usuários na máquina.

**Exploit:** Programa que explora uma vulnerabilidade em outro programa, permitindo assim que código arbitrário seja executado no sistema da vítima.

**Proxy:** Entidade que faz a mediação entre um cliente local, como um navegador web, o Mozilla, por exemplo, e um servidor na Internet. O proxy aceita os pedidos do cliente e os repassa ao servidor e retransmite então a resposta ao cliente local. O proxy pode conferir, corrigir ou simplesmente armazenar arquivos em cache, aplicar restrições de acesso e aumentar a segurança de modo geral.

**DNS:** O "Domain Name Service" (Serviço de Nome de Domínio) resolve nomes de domínio, como www.abcxyz.com, e endereços IP como 136.199.85.18. Como praticamente todos os programas de rede necessitam do DNS, falhas no serviço DNS são particularmente críticas.

**ICMP:** O "Internet Control Message Protocol" (Protocolo de Mensagens de Controle da Internet) é usado para análise de redes, por exemplo, para verificar a conexão entre duas máquinas ou descobrir o tamanho máximo permitido para um pacote. O utilitário ping informa, entre outras coisas, se um computador está ligado e acessível através de uma rede. Bombas ping podem derrubar sistemas Windows mais antigos.

para suas mensagens se você só as lê no Linux – mas pode apostar que ele não fará nenhum mal...

Nesta variante, o procmail nunca chega a ver seu email. Assim, a Listagem 2 não funcionaria. Aqui é preciso configurar um filtro diretamente em seu programa de email. A Figura 1 mostra um exemplo com o Evolution. Você pode usar o que segue com um pipe.

```
sh -c "/usr/local/bin$$
/clamassassin | grep -i $$
'x-virus-status: yes'"
```

### Listagem 2: ~/.procmailrc para o ClamAV

```
01 # Use o ClamAV para verificar
02 # se há vírus
03 :0 fw
04 | /usr/local/bin/clamassassin
05 # Encontrou vírus? Se sim,
06 # mova-o para a pasta
07 # "virus-found"
08 :0 :
09 * X-Virus-Status: Yes
10 virus-found
11 # Entregue as mensagens
12 # normalmente
```

Em outras palavras, a mensagem é mandada primeiro ao clamassassin; o grep busca palavras-chave que indicam que um vírus foi encontrado. Se essa condição for preenchida, a mensagem infectada é transferida para uma pasta de vírus especial.

### Atualizações

Como você deve ter aprendido em suas experiências com o Windows, o melhor antivírus é inútil se não for continuamente atualizado. Nesse caso, "continuamente" não significa uma atualização manual feita pelo usuário uma vez por semana, mas algo muito mais frequente.

O ClamAV traz para isso a ferramenta freshclam, um utilitário bastante profícuo que atualiza automaticamente a base de dados de assinaturas de vírus do programa. Logado como root, rode o seguinte comando:

```
/usr/local/bin/freshclam
--quiet
```

uma vez a cada hora. Você pode adicionar o comando a seu arquivo /etc/ppp/ip-up para que ele rode sempre que uma conexão PPP for aberta.

Se você tem um horário apertado, é bem sensato deixar que o daemon cron

faça esse trabalho. Para isso, acrescente a linha:

```
24 * * * * root /usr/local/bin/freshclam --quiet
```

a seu arquivo /etc/crontab. Isso atualizará a base de dados 24 minutos após cada hora cheia.

A questão final é "Esse antivírus é bom mesmo?" Para respondê-la, confira o arquivo de teste fornecido pelo projeto EICAR em [7], criado especialmente para testar programas antivírus. ■

### INFORMAÇÕES

[1] ClamAV: <http://www.clamav.net/>

[2] GNU MP: <http://www.gnu.org/directory/GNU/gnump.html> or <http://www.swox.com/gmp/>

[3] Clamassassin: <http://drivel.com/clamassassin/>

[4] Visão geral de produtos antivírus comerciais: <http://tinyurl.com/33syb>

[5] F-Prot by Frisk: [http://www.f-prot.com/products/home\\_use/linux/](http://www.f-prot.com/products/home_use/linux/)

[6] Listagens deste artigo e mais dicas de configuração: <http://www.seligma.com/linux-user/virus/>

[7] EICAR: [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)