

Ferramentas de proteção para o ambiente Linux

Quer um bom antivírus?

Analizamos os melhores programas da área, cada um com suas qualidades e defeitos. Conheça os resultados desse teste.

POR JAMES MOHR

Desde o ataque do famoso vírus *Bliss* no começo de 1997, pouco se falou na mídia sobre vírus em Linux. Contudo, dependendo de qual for sua fonte de informações, existem de algumas dúzias a até 400 vírus, trojans e outros tipos de programas maliciosos voltados para Linux e outros sistemas Unix.

Comparado com as dezenas de milhares de vírus para Windows®, as chances são muito menores de você ser diretamente atingido por um vírus de Linux. Mas, como mostrou o artigo anterior, é muito importante realizar checagens contra infecções. Se você estiver usando Linux como um servidor de email ou arquivos, precisa definitivamente considerar a instalação de um programa antivírus. No meu caso, a dúzia de vírus que pego toda semana é um motivo para tomar uma atitude ativa na luta contra essas pragas.

Ao começar esse projeto, esperava encontrar poucas companhias que oferecessem produtos antivírus para essa plataforma. Encontrei algumas que só estavam pegando carona na onda do Linux, mas muitas tinham uma atitude bastante ativa e profissional no combate aos vírus para Linux.

Nesse artigo, vou analisar alguns dos mais populares programas antivírus para Linux. Escolhi somente produtos que pude baixar na Internet e testar, mesmo que a versão fosse apenas de testes (*trial*). Não foram testados produtos

disponíveis apenas sob encomenda. Mas esse último tipo parece ser uma exceção, já que pude reunir um bom número de produtos. Em alguns casos, produtos mais avançados, como versões para servidores de arquivos ou email, não estavam disponíveis para download.

Além da capacidade de reconhecer e remover vírus em nosso laboratório de testes, também avaliei os programas por sua facilidade de uso. Tomei como princípio que a instalação e uso de um produto comercial deva ser fácil. Não deveria ser preciso um experiente administrador de sistemas para instalá-lo. Meu objetivo original era falar sobre versões para estações de trabalho (*workstation*). Mas nem toda companhia tem uma versão com essa denominação. Nesses casos, escolhi um produto com funcionalidade similar.

BitDefender

A versão Linux analisada desse antivírus foi a chamada *BitDefender-Console-Antivirus-7.0.1-3*, que vem como um arquivo *RPM*. Embora o *BitDefender* [1] não suporte a mesma gama de sistemas operacionais que programas de outras companhias, ele fornece uma boa variação em seus produtos. Há versões para o *sendmail*, para filtros específicos do *sendmail* (chamados de *milters*), *Qmail*, *PostFix* e *Courier*. Além da versão Linux, há também uma opção gratuita desse scanner para o Windows.

Embora iniciar o primeiro scan tenha sido mais simples do que em outros produtos, o único arquivo que o Bitdefender inicialmente identificou como vírus foi o arquivo de teste *EICAR*. Além disso, a ajuda online não condizia com a ajuda da página de manual. Usei um comando descrito na *manpage* que deveria incluir arquivos compactados, mas nenhum dos arquivos *.zip* foi escaneado.

O programa só foi escanear arquivos que não fossem executáveis do Windows – ou seja, terminados em *.exe*, *.com*, *.bat* – quando usei a opção *-all*. A curiosidade é que mesmo sem a opção *-all*, ele escaneou os arquivos *letter32.txt* e *body2.txt*.

Mas mesmo quando usei a opção *-all*, as coisas não funcionaram direito. O programa reportou todos os arquivos *.zip* como estando OK, enquanto outros produtos reconheceram vírus nesses arquivos. Já quando mudei as extensões para *.exe* ou *.doc*, eles foram escaneados

Listagem 1: BitDefender

```
01 Results:
02 Folders      :1
03 Files        :64
04 Packed       :0
05 Infected files :32
06 Suspected files :0
07 Warnings     :0
08 Identified viruses :7
09 I/O errors    :2
```

e identificados como compactados. E os arquivos compactados dentro deles foram identificados como os mesmos vírus reconhecidos por outros produtos.

Descobri que, no arquivo de configuração, havia uma lista de extensões que o programa usa para decidir se escaneia ou não um arquivo. Só quando acrescentei “zip” à lista, os arquivos desse tipo foram escaneados e os vírus identificados corretamente. Ao que tudo indica, se o arquivo não está na lista de extensões conhecidas, ele não é escaneado por padrão.

Considerando que o Linux não trabalha com extensões de arquivos da mesma maneira que o Windows (e esse é um scanner de Linux!), parece que o aplicativo escaneia arquivos como se estivesse no Windows, levando em conta apenas as extensões.

Mas tenho que admitir que a empresa respondeu bem rápido aos meus emails com perguntas sobre esses itens, coisa que nem toda companhia faz. Em sua resposta, admitiram que a documentação tinha que ser mais clara e foram muito atenciosos em me ajudar a resolver esses problemas. Embora eu tenha tido problemas para fazer com que o programa rodasse bem, depois que isso foi feito ele identificou todos os vírus corretamente. Já que esse é um item-chave, vale a pena considerar o BitDefender – especialmente porque a versão Linux é livre para uso doméstico.

Listagem 2: ClamAV

```
01 -----SCAN SUMMARY-----
02 Known viruses: 40507
03 Engine version: 0.86.2
04 Scanned directories: 1
05 Scanned files: 69
06 Infected files: 69
07 Data scanned: 4.91 MB
08 Time: 3.705 sec (0 m 3 s)
```

ClamAV

O *ClamAV* [2] foi o único antivírus de código aberto que encontrei. Inicialmente, imaginei que seria necessário compilar o programa, ou então que estariam disponíveis binários apenas para poucas distribuições Linux. Para minha surpresa, todas as grandes distribuições estavam cobertas, incluindo outros sistemas operacionais como *Solaris*, *AIX*, *FreeBSD* e até *BeOS*!

Havia também uma versão específica para milers do sendmail, e também para diferentes versões do Windows, tanto “nativas” quanto rodando o ambiente *Cywin*.

Baixei e instalei o RPM `clamav-0.86.2` e, ao contrário de outros produtos, as manpages foram todas instaladas corretamente. O comando `man -k clam` mostrou todas as páginas de ajuda corretas.

Meu primeiro scan foi muito simples. O ClamAV reconheceu todos os vírus, coisa que nem todo produto comercial faz. Sobre diferentes versões do produto, não há como falar de uma voltada especificamente para servidores ou estações de trabalho. Você leva o programa completo em um único pacote.

Além do tradicional scanner de linha de comando, também está incluído o `clamd`, um daemon *multi-thread* que ativa o escaneamento *on-access* (por cada acesso de arquivo) para Linux e FreeBSD. Mas isso requer que você recompile o kernel, instalando o módulo *Dazuko*.

Embora o ClamAV não seja o campeão em opções da linha de comando, ele definitivamente fica em pé de igualdade com produtos comerciais em termos de opções de configuração. Mas, infelizmente, não há um arquivo de configuração para especificar um comportamento padrão. É preciso especificar todas as opções a cada vez que se roda o programa. No entanto, escrever um *shell script* que torne isso não é difícil. Definitivamente,

não desclassifico o ClamAV por causa disso. O *clamd* e o programa de updates têm arquivos de configuração, cada um com uma grande variedade de opções.

O scanner de linha de comando possui algumas boas funções. Por exemplo, é possível escanear arquivos enviados para a entrada padrão do *clamscan* (por exemplo, `cat arquivo | clamscan -`). Outros programas terminam com diferentes códigos de saída, conforme encontrem um vírus ou ocorra algum erro. Já o ClamAV dá detalhes sobre o que aconteceu, um recurso único entre todos produtos que testei. Essas funções permitem que o programa seja facilmente integrado com outros aplicativos, por exemplo servidores de email.

F-Prot

O *F-Prot* [3], da *FRISK Software International*, talvez seja o antivírus mais famoso para Linux. Já foi o único do tipo disponível sem custo para usuários domésticos. Embora hoje já não seja o único a oferecer isso, ainda está disponível em versão integral para se usar em casa. Há também versões para Windows, algumas versões do Unix e *IBM eServers*. Baixei e instalei a versão workstation gratuita 4.6.0, disponível como um arquivo RPM.

O pacote não continha nenhum arquivo *PDF*, *README* ou coisa similar. Precisei examinar que arquivos o RPM continha para saber que tipo de documentação estava disponível e também para determinar que arquivo eu deveria executar.

Tive que adivinhar o comportamento de certas opções, já que o F-Prot tem documentação muito limitada. Embora suficiente para rodar o programa, não vai muito além disso.

A manpage faz referência a uma outra página de manual inexistente, que trata do arquivo de configuração `f-prot.conf`.

Mas o número de opções disponíveis é comparável ao de produtos comerciais e, para alguns casos, mais fácil de usar. Examinando o arquivo de configuração, encontrei opções que pareciam se aplicar apenas a um daemon ou outro programa rodando em servidores de email ou de arquivos, sugerindo que a versão gratuita é, na verdade, uma versão limitada de algum outro produto.

Todos os vírus foram identificados com exatidão pelo F-Prot. Levando em conta que reconhecer vírus é o objetivo principal, realmente vale a pena dar uma olhada nesse programa.

F-Secure Anti-Virus

O *F-Secure* [4] tem talvez a mais ampla gama de produtos antivírus; por exemplo, o *F-Secure Anti-Virus Enterprise Suite* contém produtos voltados tanto para estações de trabalho Windows como para servidores *Citrix*, *gateways* Linux, servidores *Samba* e mais.

Baixei a versão workstation 4.52, com uso limitado a 30 dias. O programa veio como um arquivo *.tgz* contendo um shell script com um binário embutido. As instruções informam que, para remover o programa, basta remover o diretório correspondente. Contudo, a remoção ainda deixa alguns arquivos pelo sistema. A documentação sugere usar o comando `find` para procurar esses arquivos, coisa pouco digna de um produto comercial.

Um ponto positivo é que, durante a instalação, você é consultado sobre diversas opções para definir o comportamento do programa. Contudo, ao contrário de outros produtos, o número de questões é mínimo.

Foi desapontador descobrir que essa versão não escaneava direito arquivos *.zip* contendo vírus. Quando isso acontecia, o programa reportava um “erro interno”. Isso aconteceu nos mesmos arquivos que versões livres e outros pro-

gramas comerciais identificaram como infectados. Para um produto comercial, não encontrar determinado vírus é algo bastante desconfortável. Não encontrei nada no site da F-Secure que pudesse me ajudar quanto a esse problema.

Além do scanner de linha de comando, há também um daemon que se inicia com um script do tipo *rc* ou pelo scanner de linha de comando. Essa versão contém um shell script que insere um *cronjob* para escanear o sistema automaticamente ou atualizar a base de dados de vírus.

AntiVir

Desenvolvido pela empresa alemã *H+BEDV Datentechnik GmbH* [5], o *AntiVir* costuma acompanhar muitas das versões do *SuSE Linux* e está disponível como download gratuito e 100% funcional para usuários domésticos. Tentei por vários dias baixar a versão Free, não-comercial, mas só obtinha erros do servidor. Acabei baixando a versão *Professional 2.1.4.8*, disponível com limite de 30 dias.

Essa impressão inicial negativa foi reforçada pelo fato de que na página da web voltada a “business solutions” o texto parecia ter sido escrito por alguém cuja língua nativa não é o inglês. Esses problemas se estendem pela documentação online e até pelo script de instalação.

Uma versão desse programa (com licença de avaliação) veio junto com a distribuição Linux que uso. Como ela já estava instalada, imaginei que a melhor maneira era removê-la primeiro para instalar a versão do site. Embora o comando `rpm`, aparentemente, tenha removido todos os arquivos, o banco de dados RPM ainda considerava o pacote como instalado.

Aparentemente, algo deve ter saído errado. Não estava clara a maneira de remover o pacote completamente. E a

Listagem 3: F-Prot

```
01 Results of virus scanning
02
03 Files: 71
04 MBRs: 0
05 Boot sectors: 0
06 Objects scanned: 129
07 Infected: 67
08 Suspicious: 1
09 Disinfected: 0
10 Deleted: 0
11 Renamed: 0
12
13 Time: 0:01
```

resposta do suporte da H+BEDV não ajudou muito.

Como não comprei a versão profissional, ela estava rodando em modo de demonstração (*DEMO mode*). Isso significa que o programa não podia atualizar as definições de vírus. Felizmente, todos os vírus que eu tinha eram velhos o bastante para já estarem incluídos. Mas se você planeja testar o produto no futuro, isso pode ser um problema.

O texto de instalação README e tudo o mais está em inglês. Mas há um documento, chamado “manual de usuário de servidores UNIX”, que está apenas em alemão, em um arquivo PDF.

Quando finalmente consegui baixar a versão *Personal Edition*, não consegui encontrar o modo de remover a versão profissional, já que ela não foi instalada na forma de um pacote RPM. A única coisa que encontrei na documentação do site indicava que um update poderia ser feito simplesmente rodando o script de instalação da versão que se deseja instalar. Foi o que fiz. O script identificou que havia uma versão já instalada e, aparentemente, fez a atualização.

Como a versão *Personal Edition* veio com uma chave de ativação, eu não mais recebia a mensagem de que se tratava de uma versão demo. Se isso é o correto ou não, não ficou claro, mes-

mo após uma troca de emails com o suporte da H+BEDV.

Em comparação com outros programas, a instalação demorou bastante, já que é preciso responder a muitas perguntas sobre como o software deve ser configurado. Para a versão profissional, isso é compreensível e até aprecio tal procedimento. Contudo, algumas das perguntas são complicadas demais para um usuário normal. Então, para a Personal Edition, esse acabou sendo mais um incômodo.

Parte do produto é o *AvGuard*, que possibilita o escaneamento *on-access* (a cada acesso de arquivo) e pede que você instale o módulo *Dazuko* através da recompilação do kernel. Esse módulo foi desenvolvido originalmente pela própria H+BEDV.

Kaspersky Anti-Virus

A versão Linux Workstation está disponível como um download, com limite de 30 dias de uso. Baixei a versão 5.5-2. Dos produtos que examinei, o *Kaspersky* [6] definitivamente passa a impressão de ser o mais profissional. Embora não queira transmitir a impressão de que os outros não sejam profissionais, esse provavelmente é o pacote mais coeso. Analisei tanto os recursos como a apresentação.

Além da versão workstation, o *Kaspersky* tem versões para servidor de

arquivos, para diversas distribuições Linux e plataformas UNIX. Uma versão para servidores de email suporta tanto o *sendmail* quanto o *Qmail*. Também há versões para *milters sendmail* e uma versão para o *Samba*. Incluído com o download, está um PDF de 68 páginas, definitivamente muito maior que a documentação dos outros produtos.

O arquivo *.tgz* que baixei continha pacotes RPM, *deb* e *tar.gz*. Instalei o RPM. Durante a instalação, pergunta-se se o módulo *Webmin* também deve ser instalado. Se você preferir, ele pode ser adicionado depois. A versão workstation também vem com um *daemon* iniciado por um *rc-script*, que intercepta requisições ao sistema de arquivos, antes que os aplicativos possam acessá-lo.

No geral, essa é uma função muito útil, mas alguns programas travaram enquanto o *daemon* estava rodando, justamente quando tentavam acessar arquivos com vírus. Também notei queda de desempenho significativa no sistema ao rodar o *kavmonitor*. Em alguns casos, a carga na CPU chegou a 100% ou ficou bem perto disso. Mas, para mim, isso não foi algo que desclassificasse o programa.

O arquivo de configuração é bem grande, com todas as opções que se pode esperar. É possível especificar a execução de determinado programa caso se identifique um vírus ou arquivo suspeito. Por exemplo, no caso de infecção, o programa pode enviar um email ao administrador, gravar um log e outras coisas do tipo. Encontrei problemas ao fazer o escaneamento como usuário normal. Baseado nas opções do arquivo de configuração padrão, não pude gravar alterações em alguns arquivos. Contudo, é possível especificar um outro arquivo de configuração e ajustá-lo para que o scanner grave em um local definido pelo usuário – desde que tenha permissões suficientes para isso.

As opções de linha de comando são assustadoras, simplesmente porque são inúmeras. Mas a documentação me deu um bom exemplo de como começar. Nem é preciso dizer que ele identificou corretamente todos os vírus. O mecanismo de update é completo, como o próprio programa, e permite fazer atualizações do banco de dados de definições, mesmo atrás de um servidor *proxy* protegido por senha.

Sophos

Esse é um antivírus oferecido pela *Sophos PLC* [7]. Encontrar a versão apropriada no site da empresa não foi uma tarefa fácil, já que precisei adivinhar que “Other” (outros) significava Linux e a maioria dos sistemas operacionais “não-Windows”. Entre eles, a maioria das distribuições UNIX, incluindo a *SCO*. Achei até uma versão para *Open VMS*.

Não ficou claro qual versão baixei, já que o arquivo se chamava `linux.intel.libc6.glibc.2.2.tar.Z`. Depois da instalação, descobri que a ferramenta principal de escaneamento estava na versão 3.97.0.

A instalação foi bem simples mas, diferentemente de outros antivírus, o *Sophos* requer que você primeiro crie, manualmente, um usuário e um grupo especiais. Depois é preciso rodar um shell script que, aparentemente, apenas copia os arquivos para o local apropriado. A remoção do produto precisa ser feita manualmente, apagando-se uma lista de arquivos e diretórios.

Fazer o primeiro scan manual não foi tão fácil, já que não estava claro que arquivo precisava ser executado. Como não havia um pacote RPM, não havia jeito de procurar por alguma manpage. Foram precisos alguns minutos para entender o que precisava ser feito.

Embora tenha instalado o programa como usuário *root*, acabei com um mon-

Listagem 4: Sophos

```
01 67 files swept in 2 seconds.
02 2 errors were encountered.
03 60 viruses were discovered.
04 60 files out of 67 were infected.
05 Please send infected samples
for Sophos for analysis.
06 For advice consult www.sophos.com,
email support@sophos.com or
telephone +44 1235 559933
07 End of Sweep.
```

te de problemas quando tentei fazer meu primeiro escaneamento. Havia um diretório ausente, requerido pelo programa. Depois de criar esse diretório, descobri que faltava um outro. Após passar por esse processo mais algumas vezes, finalmente consegui rodar o scan.

O motivo de esses diretórios estarem faltando não estava explicado em nenhum lugar do site da Sophos. Tive uma resposta bem rápida da empresa quando enviei um email perguntando sobre isso; foram bastante atenciosos em me ajudar. Depois disso, o scan rodou fácil e a ferramenta rapidamente identificou alguns vírus. Contudo, cinco dos arquivos foram deixados de lado e a ferramenta não identificou os vírus de outros cinco arquivos. Ao usar a opção `-all`, aparentemente alguns tipos de arquivo não foram escaneados. Para escanear todos meus arquivos infectados, precisei usar tanto a opção `-all` quanto `-archive`.

Tentei entender quais tipos de arquivos não eram escaneados por padrão. Também tentei usar diferentes opções para que arquivos limpos fossem listados, sozinhos ou como parte de um arquivo de registro completo, sem sucesso. Embora tenha conseguido, em determinado momento, que todos os arquivos fossem escaneados e seus vírus, detectados, isso deu muito trabalho.

Vexira

Esse é um produto fornecido pela empresa *Central Command, Inc.* Baixei a versão 1.2.0 do *Vexira Command Line Virus Scanner* [8].

Na verdade, o Vexira não é "instalado" no sentido tradicional do termo. Você simplesmente descompacta o pacote e tem todos os arquivos necessários na sua frente. Embora isso possa ser interessante em um programa livre para uso pessoal, fiquei desapontado por se tratar de um produto profissional.

Em comparação com outros produtos, não há muitas variações no Vexira Antivírus. Existe uma opção para servidores de email, Samba e um produto voltado simplesmente para "servidores Linux".

Já de início, senti que sua linha de comando é ligeiramente pesada e lenta. Ao executar o comando, não fica imediatamente óbvio quais as opções – e em que ordem usá-las – precisam ser fornecidas simplesmente para se escanear e listar arquivos infectados. Por padrão, a ferramenta pára em qualquer arquivo infectado e pergunta o que fazer.

Minha opinião pessoal é que, ao escanear o sistema, o usuário simplesmente quer saber se há vírus antes de tomar qualquer atitude. Ter que responder o que fazer em cada arquivo infectado é um pouco irritante. Como computadores já são bens bastante difundidos, seria de se esperar que as coisas simplesmente funcionassem de maneira suficientemente fácil. Não deveria ser necessário ler toda a documentação disponível apenas para um scan básico.

Diferentemente de outros produtos, o Vexira não tem update automático das definições de vírus. É preciso acessar um servidor FTP para baixar e instalar o banco de dados manualmente, substituindo as definições antigas. Mas uma coisa de que realmente gostei foi o relatório do scan.

A cada vírus que encontra, ele mostra um *killable* (exterminável) ou *Not killable*, por exemplo. Além disso, soma os diferentes tipos de programas maliciosos encontrados, como vermes de Internet, vírus ou até mutantes. Isso me pareceu realmente único em um antivírus. Apesar dos pontos negativos que encontrei no programa, fiquei com uma boa impressão sobre o produto, tanto do ponto de vista técnico quanto em relação à empresa de modo geral. Recebi respostas bem rápidas aos meus emails com dúvi-

Listagem 5: Vexira

```
01 Summary of scanned objects' types
02 -----
03 files (total)      | 68
04   in archives     | 59
05   mail parts      | 6
06
07 Summary of malware pieces found
08 -----
09 iworm              | 67
10 virus              | 3
11 mutant             | 1
12
13 Summary of actions taken on alert
14 -----
15 skipped            | 71
16
17 Error summary
18 -----
19 inaccessible target | 2
```

das, e os técnicos estavam abertos tanto para sugestões quanto críticas.

Sem solução única

Não pude encontrar um produto específico que fizesse tudo direito. Como costuma ser o caso com software, é preciso tomar uma decisão com base nos recursos mais importantes para você. Os produtos que imediatamente reconheceram todos os vírus talvez tenham características que não lhe agradem. Dependendo das necessidades de cada usuário, um produto pode ter um recurso que o faz sobressair-se dentre os outros.

INFORMAÇÕES

[1] Bitdefender: www.bitdefender.com

[2] Clam AV: www.clamav.net

[3] F-Prot: www.f-prot.com

[4] F-Secure: www.f-secure.com

[5] H+BEDV: www.hbedv.com

[6] Kaspersky: www.kaspersky.com

[7] Sophos: www.sophos.com

[8] Vexira: www.centralcommand.com

