

O KlamAV leva o antivírus ClamAV para seu desktop KDE

Clamando por segurança



www.sxc.hu - Linda McNally

Linux pode não ser vulnerável como o Windows, mas nenhum usuário quer ficar “hospedando” programas maliciosos. Está aberta a temporada de caça aos vírus com o KlamAV, um front-end para o sistema de proteção de código aberto ClamAV.

POR ROBERT HOGAN

Se você recebe email e baixa arquivos de fontes não confiáveis, seu computador pode acabar se tornando um “repositório” de vírus e programas maliciosos. Embora muito poucos desses programas possam causar danos reais a um sistema Linux, esses vírus continuam sendo desnecessários e indesejados. Em alguns casos, existe o risco de transmitilos para usuários de Windows®. Portanto, faz sentido implementar alguma forma de proteção.

Uma das maiores histórias de sucesso envolvendo software livre é o *ClamAV*, que busca por assinaturas de vírus em servidores de email, desenvolvido originalmente por Tomasz Kojm e hoje apoiado por uma comunidade crescente, com infra-estrutura de atualizações de nível profissional. Já o objetivo do *KlamAV* é trazer esse poderoso sistema para o desktop *KDE*.

Obtendo ClamAV/KlamAV

O KlamAV já está começando a vir com algumas distribuições Linux populares. Se o programa não estiver disponível em seu sistema, é possível instalá-lo de diversas maneiras. A primeira opção é o instalador disponível em [1]. Um duplo clique no arquivo baixado irá descompactar e rodar um programa chamado *Arkollon* [2], que gerencia a compilação e instalação do KlamAV e seus componentes. Mas a instalação manual também é uma opção, se você tiver baixado o pacote com o código fonte. Nem é preciso dizer que o ClamAV é um pré-requisito para o KlamAV. Então, não se esqueça de baixá-lo [3] e instalá-lo antes de tudo.

Escaneando arquivos e diretórios

A aba *Scan* da janela principal do KlamAV permite selecionar os arquivos e pastas que se deseja escanear. Todas as pastas de seu sistema estão disponíveis nessa aba. É possível selecionar qualquer combinação de diretórios, com qualquer

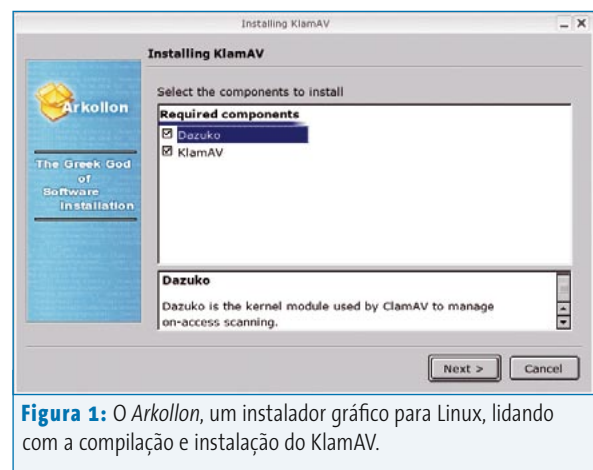


Figura 1: O Arkollon, um instalador gráfico para Linux, lidando com a compilação e instalação do KlamAV.

número de níveis, em quantas árvores de diretórios você quiser, em um único passo. O KlamAV pode rodar vários scans ao mesmo tempo.

Você também pode dar um clique com o botão direito do mouse em um arquivo ou diretório no *Konqueror* e começar um scan pelo menu de contexto do navegador de arquivos. O KlamAV irá abrir uma nova aba de escaneamento e continuará com os processos interrompidos. Ainda no espírito de completar tudo de uma vez só, é possível agendar scans futuros nessa janela: por exemplo, após seu próximo login no KDE.

Um recurso popular em muitos antivírus comerciais é a checagem *on-access*, ou seja, o escaneamento automático de arquivos assim que são acessados pelo sistema. Graças ao módulo do kernel *Dazuko* [4] e o suporte integrado do ClamAV a esse recurso, a checagem *on-access* também é possível via KlamAV.

O Dazuko intercepta chamadas do sistema a arquivos e permite que programas externos, como o ClamAV, decidam se o acesso a esse arquivo deve ser permitido. Convenientemente, ele vem junto com o KlamAV. No entanto, como o kernel varia conforme a distribuição, talvez seja melhor não selecioná-lo na hora da instalação e fazer isso manualmente mais tarde.

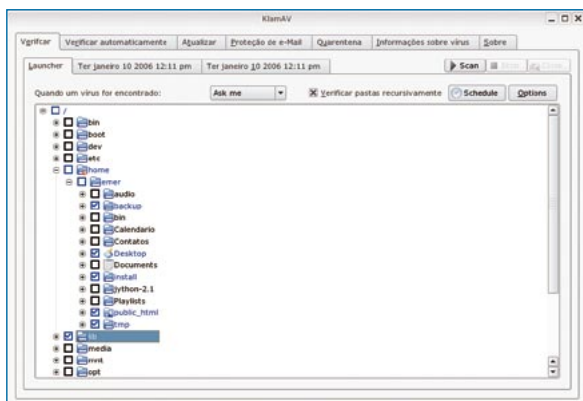


Figura 2: Selecionando diretórios para serem escaneados. Note que há scans em andamento nas abas de seções ocultas.

A configuração é simples e direta. Você pode decidir sob quais condições os arquivos serão escaneados (por exemplo, no momento da execução, abertura, fechamento, leitura ou gravação do arquivo). Se quiser usar esse recurso, encontre a combinação que melhor satisfaça a suas necessidades. Mas mantenha-se consciente de que esse é, talvez, o elemento mais experimental do ClamAV/KlamAV. Nem toda a área de escaneamento *on-access* no Linux está 100% madura.

Verificando emails

Uma desvantagem irritante nos atuais sistemas desktop do Linux é que a maioria das tentativas para escanear novos emails trava completamente o cliente de email enquanto as mensagens são baixadas. Mas graças à elegância da arquitetura ClamAV, o KlamAV oferece um componente chamado *kscanmail* para corrigir esse problema.

Trata-se basicamente de um utilitário de linha de comando que aceita email na entrada padrão, faz o escaneamento em um processo ClamAV rodando no fundo e o devolve na saída padrão. Uma vez que o processo de scan roda como um daemon, não há grande perda de tempo com a inicialização do *kscanmail*.

Caso o email esteja infectado, o *kscanmail* isola o vírus em um email de alerta e mostra uma janela de aviso. Para usar esse útil recurso, selecione a aba *Proteção*

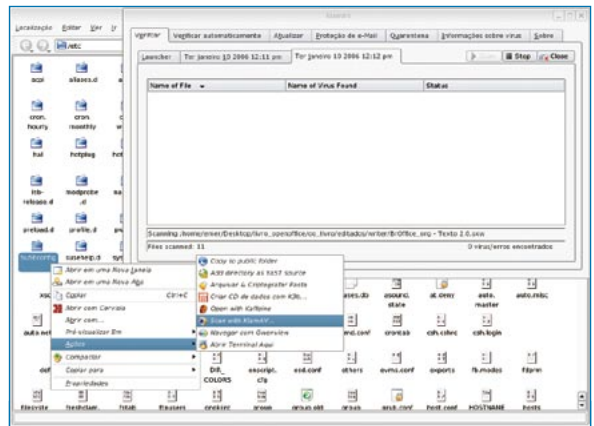


Figura 3: Enquanto a checagem é feita, você pode selecionar outros arquivos e diretórios para escanear a partir do *Konqueror*.

de e-Mail no KlamAV e peça para ele configurar seu cliente de email para a verificação de novas mensagens. Caso seu cliente de email não seja compatível com a configuração automática, o KlamAV permite configurar manualmente qualquer cliente de email em que seja possível “dar um *pipe*” nas mensagens para um programa externo. Estão disponíveis instruções para guiá-lo por esse processo de configuração.

Atualizações

A parte mais importante do gerenciamento de um sistema de proteção para desktop é manter-se atualizado. O ClamAV possui uma rede de atualizações que fica em pé de igualdade com – e muitas vezes até superando – opções comerciais, em velocidade e precisão na resposta a vírus descobertos. Um estudo recente da *Electric Mail* constatou que, comparado com dois dos cinco melhores antivírus comerciais,

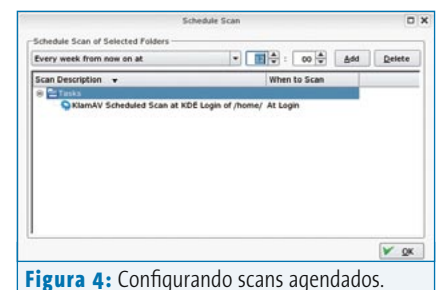


Figura 4: Configurando scans agendados.

o ClamAV foi o primeiro a responder em 77% das vezes em que foram descobertos os últimos 50 novos vírus [5].

O KlamAV também permite o contato “permanente” com o serviço de atualização com apenas alguns cliques. Para checar por atualizações a cada meia hora, simplesmente selecione a aba *Atualizar*, selecione *48 Vezes por dia* e marque *Atualizar base de dados de vírus automaticamente*. Agora clique em *Atualizar agora* e esqueça o que acaba de ler, pois não vai precisar disso de novo.

Além das atualizações no banco de dados de assinaturas de vírus, também é importante manter o próprio ClamAV atualizado. Seu “motor” contém importantes sistemas de detecção, que são continuamente melhorados e atualizados. Se você selecionar *Update ClamAV automatically* (a tradução em português está incompleta) na aba *Atualizar*, o KlamAV irá checar por uma nova versão do ClamAV sempre que ele for iniciado. Se uma nova versão estiver disponível, ela será baixada e até compilada. Mas mesmo que essa opção não seja marcada, o programa ainda vai alertá-lo de que sua versão está ultrapassada, oferecendo a opção de baixar e instalar a atualização.

Vírus encontrado! Não entre em pânico

Não há muito segredo para se encontrar vírus. A tarefa desafiadora é decidir o

que fazer com arquivos suspeitos. Isso porque os nomes dos vírus são pouco esclarecedores. Todo mundo, em algum momento, já se viu no *Google* buscando pelo significado de nomes como “Gen.1024-PrScr.1”.

O KlamAV tenta integrar da maneira mais fácil possível esse segundo passo no procedimento da descoberta de um vírus em seu sistema. Quando o KlamAV encontra um vírus, ele é mostrado na interface de escaneamento. Você tem a opção de deixar todos os arquivos suspeitos em quarentena imediatamente (eles podem ser investigados melhor mais tarde, na aba *Quarentena*) ou usar o botão direito do mouse para selecionar um ou mais arquivos para uma pesquisa específica e a “internação” em quarentena.

Se o ClamAV achar uma versão do *Worm.Mytob*, por exemplo, você pode selecionar *Search Worm.Mytob with VirusPool*. Essa opção irá abrir a aba *Informações sobre Vírus*. O banco de dados de assinaturas de vírus vai aparecer e um navegador embutido exibirá informações sobre o Mytob usando como fonte o *VirusPool*, um banco de dados online sobre vírus conhecidos.

Enquanto estiver no navegador de vírus, você pode pesquisar qualquer um dos vírus no banco de dados do ClamAV usando diferentes fontes online. A opção de pesquisar vírus também está disponível no gerenciador de quarentena, novamente com um clique do botão direito do mouse sobre o arquivo infectado.



Figura 6: Cheque o banco de dados de assinaturas com o navegador de vírus do KlamAV.

Finalmente

O KlamAV é o humilde primo para KDE do formidável ClamAV. Ele traz todo o poder do ClamAV para o KDE, com uma interface em que é muito fácil verificar arquivos e gerenciar suspeitas de infecções. O futuro dos sistemas antivírus e de proteção contra programas maliciosos para o desktop no Linux aponta para diversas direções. Entre elas, detecção de *root kits*, análise heurística, a evolução do scan on-access e do escaneamento da memória residente.

Essa área vai se tornar mais importante junto com o crescimento da adoção do Linux. E o ClamAV certamente fornece uma boa base para satisfazer as necessidades do usuário doméstico de Linux. Vamos torcer para que o KlamAV continue em sua missão de oferecer um ótimo antivírus para o KDE. Se quiser ver o KlamAV em ação, vá até o site e cheque o vídeo-tutorial. Ou mergulhe logo de cabeça e baixe o instalador em [1]. ■

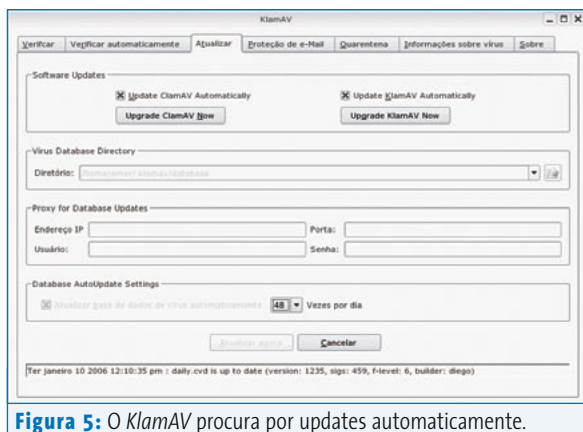


Figura 5: O KlamAV procura por updates automaticamente.

INFORMAÇÕES

- [1] KlamAV: klamav.sf.net
- [2] Arkollon: apollon.sf.net
- [3] ClamAV: www.clamav.net
- [4] O Dazuko está disponível em: www.dazuko.org
- [5] Estudo da Electric Mail: www.linuxpipeline.com/166400446