
Cory LaFlame – www.sxc.hu

Filtrando vírus e outras ameaças

Rede de Intrigas

Integrar um anti-vírus ao seu servidor proxy é mais simples do que parece. Veja as alternativas e aumente a segurança de sua rede.

por Augusto Campos

Embora a avassaladora maioria dos vírus sejam feitos para Windows®, os administradores de sistema Linux – não sem uma ponta de ironia - dedicam boa parte do seu tempo a lidar com esta ameaça, já que têm a oportunidade de barrá-la nos servidores de e-mail que administram, antes que alcancem o usuário final e possam causar o dano para o qual foram planejados.

Mas já faz algum tempo que os autores de vírus de computador perceberam que a disseminação de suas criações estava sendo barrada com eficácia cada vez maior pelos servidores de e-mail integrados a programas anti-vírus, e começaram a produzir métodos alternativos, como o *phishing*, em que um e-mail malicioso não traz cópia do vírus, e sim um link para ele – acompanhado de um texto apelando para motivos diversos (de fotos curiosas a avisos de débitos ou prêmios inexistentes) tentando convencer o usuário a clicar e instalar o vírus. Infelizmente este método mais sutil funciona bem, é mais difícil de detectar, e em conseqüência as infecções continuam crescendo.

É neste ponto que surge o próximo patamar na escalada contra os vírus: os antivírus de proxy web. O esquema de funcionamento é relativamente simples: todos os downloads via web passam a ser interceptados (geralmente por um servidor proxy "genérico" como o *Squid* [1]) e transferidos a um programa de controle, que usa um antivírus comum (sugestão: conheça o *ClamAV* [2], que é livre) para garantir que os arquivos não estão contaminados. Este método tem outro efeito positivo: serve também para combater os vírus de e-mail comuns transmitidos via webmails externos.

Instalar e configurar o Squid é uma tarefa bem documentada e relativamente trivial, mas que vai muito além do escopo deste artigo. As minhas dicas deste mês têm um alvo bem mais específico: os administradores de sistema que já contam com um servidor proxy configurado, e ainda não sabiam que é fácil integrar um antivírus a ele.

Neste sentido, a opção mais conhecida é o *Viralator* [3], um script em Perl que se integra ao Squid recebendo todos os fluxos de download e repassando-os ao antivírus que você tiver instalado incluindo, além do ClamAV, algumas opções comerciais como o McAfee, Trend e Sophos. Dependendo do resultado da inspeção, o arquivo tem seu download completado, passa por um processo de limpeza ou é removido automaticamente.

Recentemente surgiu mais uma opção interessante neste cenário: o *HAVP* (HTTP Anti Virus Proxy). Seu principal diferencial em relação ao Viralator é ser um proxy completo, e não apenas um script que complementa o proxy existente (embora isto não o impeça de operar em conjunto com o Squid). A principal conseqüência desta diferença é a maneira contínua com que ocorre o processo de verificação, sem que a barra de progresso do navegador do usuário final apresente paradas bruscas. Se você quiser dispensar o Squid, o HAVP tem suporte até mesmo a recursos avançados como proxy transparente e participação em hierarquias.

Ambos os programas são capazes de lidar com truques comuns como sites protegidos por senhas ou nomes de arquivo com caracteres especiais. O Viralator está em um estágio mais avançado de desenvolvimento, mas o HAVP tem características superiores e certamente merece sua atenção. Experimente, os usuários de sua rede vão agradecer. ■

Informações

[1] Squid: www.squid-cache.org
[2] ClamAV: www.clamav.net
[3] Viralator: viralator.sourceforge.net
[4] HAVP: www.server-side.de