# Rootkit infecta servidores Linux

Um rootkit desconhecido tem infectado servidores Linux e injetado códigos maliciosos em suas páginas. O rootkit foi descoberto por um usuário da lista de discussão *Full Disclosure*, que publicou suas observações, assim como o módulo kernel suspeito. O malware adiciona um iframe para cada página servida pelo sistema infectado através do proxy `nginx` – incluindo páginas de erro.

Qualquer pessoa que visita uma página no servidor é atacada por outra, carregada via iframe. Criminosos costumam utilizar exploits como o BlackHole para examinar o sistema da vítima e estabelecer qual das séries de vulnerabilidades do Flash, Java e outros aplicativos podem ser exploradas. Uma vez que um buraco explorável é identificado, é utilizado para instalar um malware no sistema do visitante; o servidor é então usado para redirecionar os usuários para outro servidor que infecta com malware sistemas que possuam manutenção deficiente, como é o caso do Windows.

A empresa de software antivírus Kaspersky Lab analisou o malware. Segundo eles, o rootkit, que duplicou o `Rootkit.Linux.Snakso.a`, é projetado para atacar sistemas de 64 bits e foi compilado para a versão do kernel 2.6.32-5, usado no Debian Squeeze. O rootkit adiciona a linha `insmod /lib/modules/2.6.32 5-amd64/kernel/sound/module_init.ko` no script `/etc/rc.local`, garantindo que o módulo malicioso seja executado cada vez que o sistema for inicializado. Após a inicialização, ele determina o endereço de memória de uma série de recursos do kernel, aos quais se encaixa em seguida. Isto permite ao rootkit tanto esconder-se do usuário como manipular o tráfego de rede do servidor, além de obter instruções de implementação de um servidor de comando e controle. Segundo a Kaspersky Lab, o rootkit pode estar ainda em desenvolvimento, já que foi compilado com informações de depuração. ■

# CyanogenMod 10 oferece atualizações "pelo ar"

Os desenvolvedores do projeto CyanogenMod anunciaram em meados de novembro de 2012 a primeira versão estável do CyanogenMod 10 (CM10), baseado no Android 4.1 "Jelly Bean". A versão mais recente da ROM alternativa para dispositivos Android inclui muitas características do Jelly Bean, bem como alguns desenvolvimentos personalizados feitos pela equipe do CyanogenMod, como um novo gerente de atualização e ajustes para a interface do usuário. Os desenvolvedores também detalharam os planos para integrar as mudanças do Google para o Android 4.2.

O espelhos do projeto não incluem atualmente imagens do CM10 para todos os dispositivos suportados, já que estão em processo de construção, mas as imagens faltantes devem aparecer em breve. Na versão mais recente, o CyanogenMod muda para um novo gerenciador de atualização que permite aos usuários receber atualizações pelo ar, sem a necessidade de um aplicativo terceiro, como um gerenciador de ROM (ROM Manager).

No anúncio, os desenvolvedores afirmaram que já estão atentos para as mudanças introduzidas no Android 4.2 e planejam incorporá-las em uma versão futura do CyanogenMod 10.1. Isso permitirá que usuários de aparelhos como o Nexus S obtenham acesso potencial aos recursos do Android 4.2, devido ao fato de o Google ter anunciado que nem todos os dispositivos receberão uma atualização com base na versão 4.2. ■

## Lançado o ROSA Enterprise Linux Server 2012

A empresa russa ROSA, anteriormente conhecida pelo Mandriva-fork ROSA Marathon 2012, acaba de lançar o *ROSA Enterprise Linux Server (RELS) 2012*, sob o codinome "Helium". Em contraste com o ROSA desktop, o servidor de distribuição não é baseado no Mandriva, mas no Red Hat Enterprise Linux (RHEL) 6 e possui vários pacotes adicionais, ferramentas próprias e aplicativos.

O RELS inclui um componente de diretório, o ROSA Directory Server, para gerenciamento de recursos e usuários. Há também uma interface administrativa online, o ROSA Server Setup, para instalar e configurar componentes, tais como MySQL, PostgreSQL, Samba, CUPS, Postfix e Bacula. O servidor de distribuição usa o kernel Linux 2.6.32 e inclui o LXDE como desktop padrão, juntamente com uma série de ferramentas agregadas. Desktops GNOME 2.28 ou KDE 4.3.5 também podem ser opcionalmente instalados. Além disso, o RELS inclui o recém-lançado OpenStack Essex, de modo que a distribuição também pode ser utilizada para configurar ambientes IaaS em nuvem ("infraestrutura-como-serviço").

O ROSA Enterprise Linux Server "Helium" 2012 está disponível para download em sistemas 32-bit e 64-bit de espelhos do ROSA. Usuários que se cadastrarem no site oficial receberão 30 dias de suporte grátis. Os desenvolvedores da distribuição prometem atualizações de segurança rápidas, mas se reservam ao direito de limitar outras melhorias na distribuição para clientes que pagarem por elas. ■

## Linguagem de programação Go completa 3 anos

O projeto de código aberto Go celebrou seu terceiro aniversário neste fim de semana. Desde que a linguagem de programação foi anunciada pelo Google, em novembro de 2009, o projeto tem tido o apoio de centenas de colaboradores externos em todo o mundo. Organizações que utilizam a linguagem incluem atualmente a BBC, a Novartis, SoundCloud, SmugMug e Canonical, entre outras. O próprio Google tem utilizado o Go para fornecer bits lógicos para vários de seus Doodles interativos.

Os desenvolvedores atualmente trabalham na versão 1.1 da linguagem, após terem lançado a primeira versão estável do Go em março deste ano. O Go 1.0 trouxe uma estabilização da linguagem que possibilitou sua utilização em larga escala. O Go agora inclui um sistema de gerenciamento de pacotes e é compatível com o *Google App Engine*. Mais informações sobre a linguagem encontram-se disponíveis nas páginas de documentação do projeto. O Go está sob uma licença BSD e o código fonte para o projeto está hospedado no Google Code. ■