O código-fonte do Android 4.0

O Google disponibilizou o código-fonte do novo Android 4.0, batizado de *Ice Cream Sandwich* (ICS), conforme havia prometido quando lançou a nova versão do sistema operacional para dispositivos móveis. Jean-Baptiste Queru, engenheiro de software do Google no *Android Open Source Project* (AOSP), anunciou na lista de discussão oficial, a *Android Building Google Group* que o código-fonte estava sendo atualizado nos repositórios. Ele ressaltou que o código que está sincronizado nos repositórios correspondem à versão 4.0.1, que é a versão específica do sistema operacional que será fornecido juntamente com o smartphone Galaxy Nexus.

Os respositórios agora também conterão o código-fonte para as versão 3.x Honeycomb do Android, mas ele estará espalhado pelo histórico dos vários arquivos. O Honeycomb não teve seu código disponibilizado porque, de acordo com o Google, ele continha uma série de soluções impróprias (hacks) para que pudesse funcionar em tablets. De acordo com Queru, o Honeycomb é um sistema que o Google considera incompleto e o foco do trabalho de todos deve ser a versão Ice Cream Sandwich.

O código-fonte do ICS pode ser compilado para o Galaxy Nexus, contudo, espera-se que outros dispositivos sejam acrescentados aos repositórios oficiais nas semanas vindouras, além disso, outros desenvolvedores podem começar a criar ROMs personalizadas para seus dispositivos agora. A disponibilidade do código-fonte antes do lançamento de qualquer aparelho é uma melhoria considerável, se comparada à disponibilização dos códigos-fonte anteriores e possivelmente podem definir um novo padrão para as edições futuras do Android.

Instruções gerais para o download da árvore de código estão disponíveis para os interessados e, de acordo com Queru, o comando para a atualização e download do código no repositório para uma máquina local deve ser `repo init -u https://android.googlesource.com/platform/manifest -b android-4.0.1_r1` ■

Envenenamento de DNS nos provedores brasileiros

Apesar do silêncio da mídia brasileira, sites internacionais de segurança deram durante a primeira quinzena de outubro, atenção especial a recentes ataques que redirecionaram o cache DNS de provedores brasileiros de acesso à Internet, que redirecionaram os usuários para a instalação de malwares. Os ataques, documentados em uma entrada do blog Securelist, da Kapersky [1], faziam com que os usuários que digitassem "www.google.com.br" em seus navegadores fossem direcionados à um site que lhes contava que para usar o site de buscas eles deveriam instalar o software falso "Google Defence". O programa não passava de um trojan bancário e o site em que o arquivo estava hospedado também incluia arquivos executáveis (.exe) que fingiam ser programas de configuração para o Facebook, Youtube e outros sites populares.

A Kaspersky apontou que, depois de descobertos esses ataques, a Polícia Federal brasileira prendeu um funcionário de 27 anos de um provedor de médio porte do sul do país que fora acusado de participar dos esquemas de envenamento de cache. Ele já vinha modificando o cache de DNS do provedor e redirecionando usuários para o site malicioso há pelo menos dez meses.

Um provedor típico no Brasil possui entre 3 e 4 milhões de clientes, fazendo com que seus caches de DNS sejam um alvo valioso; essa mudança de cache em apenas um servidor poderia enviar dezenas de milhares de usuários para sites de criminosos em que podem ser enganados a instalar malwares. O sistema de DNS permite que nomes de domínios sejam traduzidos em endereços IP, o sistema pode realizar a busca dos endereços de domínio com consultas aos servidores DNS e recebendo a tradução adequada dos nomes em endereços numéricos. Como essa consulta pode demorar algum tempo, os servidores de DNS armazenam os resultados de pesquisas em caches por um período de tempo. O envenamento de cache DNS corrompe esses dados armazenados colocando endereços IP diferentes, normalmente para sites hospedando aplicativos maliciosos.

[1] Blog Security List: http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil ■

IBM sob nova direção

A IBM não gosta de reviravoltas dramáticas, e provou isso quando, sem qualquer estardalhaço, nomeou a veterana com trinta anos de casa, Virginia Rometty, para suceder Sam Palmisano como CEO da empresa no final de outubro de 2011.

O antecessor de Rometty foi uma figura reservada no mundo de TI, não buscou os holofotes em Washington ou no Vale do Silício, mas que sem dúvida trouxe grandes mudanças para a IBM e colocou a empresa em rumo certo e definido. Rometty, que ocupa até então o cargo de vice-presidente Sênior e Executiva de grupo para Vendas, Marketing e Estratégia da companhia, vai assumir como CEO no dia primeiro de janeiro de 2012. Palmisano deve permanecer como presidente do conselho.

Rometty se juntou à IBM em 1981 como engenheira de sistemas. Em 2002, sua atuação se tornara especialmente relevante quando acompanhou a integração da PricewaterhouseCoopers e seus 100.000 consultores na empresa, após a aquisição da gigante em consultorias pela IBM, por 3,5 bilhões de dólares.

A decisão foi considerada por analistas uma confirmação das tradições da IBM, que coloca a empresa, e não a pessoa de um executivo, em primeiro lugar. Eles consideram que Rometty possui bom conhecimento e compreensão dos negócios de software, serviços e hardware da empresa e que não devem esperar grandes mudanças de administração. ■

Riverbed entra para a comunidade OpenStack

A Riverbed Technology, empresa de alto desempenho em TI, anuncia a sua participação na comunidade OpenStack, um grupo global de desenvolvedores que trabalha de forma colaborativa em prol de um sistema operacional para nuvem baseado em código aberto.

Com as empresas migrando os seus dados e aplicativos para a nuvem, a crescente conectividade via rede WAN (geograficamente dispersa) apresenta-se como um desafio para o desempenho dos aplicativos. Como membro da OpenStack, a Riverbed também está trabalhando com o grupo nas suas próprias soluções de otimização da WAN a fim de viabilizar ambientes em nuvem bem-sucedidos.

O trabalho da OpenStack com as soluções Riverbed para otimização da WAN é uma expansão de uma colaboração anterior com esta comunidade, relacionada à controladora para a entrega de aplicativos virtuais (vADC). As soluções Riverbed para otimização da WAN e as vADCs dão às empresas uma plataforma tecnológica que melhora o desempenho em ambientes de nuvem pública, privada e híbrida.

Mais de 16 mil empresas mundialmente usam Riverbed para entender, otimizar e consolidar as suas infraestruturas de TI, através de soluções que respondem aos desafios de desempenho relacionados à distância, ao ambiente distribuído e ao crescente volume de dados. Com as áreas de TI adotando iniciativas estratégicas para virtualizar, consolidar e migrar as cargas de trabalho para o ambiente em nuvem, os usuários levam seus dados para mais longe. Dessa forma, os aplicativos e as transferências de arquivos ficam mais lentos e os sites – que se tornam ineficientes – interferem negativamente no desempenho dessas iniciativas.

A Riverbed melhora substancialmente o desempenho de TI com soluções que abrangem otimização da WAN , gerenciamento do desempenho da rede (NPM) com base na entrega dos aplicativos, otimização de conteúdo web (WCO), proteção dos dados em nuvem para backup, arquivamento e recuperação de desastres. Oferecendo amplo portfólio de soluções de desempenho que otimizam qualquer aplicativo, onde e quando necessário, a Riverbed permite que as empresas melhorem a produtividade, a eficiência, a flexibilidade dos negócios e controlem os custos. ■