Falha 'mais grave' do Linux é usada para infectar celulares Android

Renato Santino 26/09/2017 21h40 Android Google Google Play

Usuários de Android já estão familiares com diversos ataques mirando seu sistema operacional de escolha, ainda que possivelmente nunca tenham sido atingidos por um deles. Agora foi descoberta uma nova ameaça em uso ativo pelo cibercrime que permite a obtenção de root no celular sem autorização, dando acesso total ao aparelho.

A vulnerabilidade ficou conhecida como Dirty Cow ("Vaca Suja" em português) e foi revelada em outubro do ano passado. Ela estava escondida desde 2007 no kernel do Linux, usado também como núcleo do Android, e só foi solucionada no final do ano passado. A questão é que, como fabricantes e operadoras demoram tanto para liberar atualizações para o Android (quando soltam), existem inúmeros celulares que ainda estão vulneráveis.

Quando a falha foi descoberta, no final de 2016, ela já estava em uso para atingir servidores Linux, sendo considerada uma das brechas mais graves da história do sistema. Poucos dias depois especialistas já estavam usando a vulnerabilidade para realizar root no Android. Agora foi descoberta uma campanha massiva usando essa técnica pelo cibercrime.

Segundo um estudo da empresa de segurança Trend Micro, já há mais de 1.200 aplicativos disponíveis em lojas alternativas (fora do Google Play) usando a Dirty Cow. A ideia é cadastrar a vítima em serviços pagos via SMS, que acabam causando prejuízos financeiros que podem ser grandes. Até o momento, foram pelo menos 5.000 infecções em 40 países diferentes, sendo a maioria dos casos na China e na Índia por uma família de aplicativos chamada de ZNIU (a lista completa está aqui). Esses apps também burlam as restrições do sistema e deixam uma porta aberta para que os criminosos possam acessar o dispositivo para outros ataques posteriores.

A vulnerabilidade não deve atingir pessoas que tenham recebido o pacote de segurança liberado mensalmente pelo Google referente a dezembro do ano passado. O problema é o percentual desconhecido do público que teve acesso a essa correção. O pesquisador David Manouchehri estima que é provável que os aparelhos que usem uma versão do Android inferior à 5.1.1 estejam vulneráveis, mas nada impede que aparelhos mais novos também estejam. Segundo os números mensais do Google, cerca de metade dos usuários do sistema ainda usam versões inferiores à 5.1.1 e a empresa não tem uma estimativa de quantos modelos receberam e instalaram o pacote de dezembro.

Aparelhos muito antigos, no entanto, se beneficiam de uma peculiaridade deste ataque. Segundo o estudo, a ameaça só afeta aparelhos com processador com arquitetura ARM ou x86 de 64 bits. Desta forma, boa parte dos usuários das versões mais antigas do Android acabam protegidos dessa ameaça específica, uma vez que seus processadores são de 32 bits apenas.