

27 January 2012

Novo ataque aos utilizadores de Android

Os atacantes publicam aplicações legítimas que posteriormente trocam por malware depois de ter obtido as qualificações positivas

A Bitdefender®, galardoado provedor de soluções inovadoras de segurança para a Internet, localizou um novo ataque informático contra os utilizadores do sistema operativo Android.

Neste caso, a campanha desenhada pelos ciber-delinquentes consiste em publicar aplicações legítimas para Android em páginas online de outros para atrair os utilizadores e incentivá-los a que as instalem e as valorizem. Depois, quando tenham obtido valores positivos, manipulam-nas com o fim de instalar nos smartphones dos utilizadores serviços maliciosos juntamente com a aplicação original.

Assim, um utilizador que descarregue uma aplicação original para Android através de um destes sítios obterá uma aplicação verdadeira, assim como um serviço trojanizado (normalmente designa-se de "GoogleServicesFrameworkService"), que se inicia assim que o programa começa a ser utilizado.

Identificado pela Bitdefender como Android.Trojan.FakeUpdates.A, este exemplar de malware liga-se a um servidor C&C e obtém uma lista de links para APK's (Android Application Package, um pacote de aplicações para o sistema operativo Android) diferentes. Depois disso, descarrega cada APK e apresenta uma notificação com o texto "Para ter acesso às últimas actualizações, faça clique em Instalar" (até agora apenas em línguas asiáticas). Isto confunde o utilizador que não sabe de onde provém a mensagem.

Este trojan pede uma ampla gama de permissões enquanto se instala, com o intuito de se assegurar de que pode tomar o controlo total sobre o telefone inteligente quando seja necessário. Dependendo da APK's que descarregue e instale, a aplicação pode requerer até 10 autorizações antes da instalação e a maioria dos utilizadores aceita-las sem nenhum tipo de dúvidas, já que acreditam que o que vão instalar é uma actualização de uma das aplicações que já tinham descarregado.

"A publicação de aplicações para Android em páginas de outros não são nada de novo, contudo, o que é particularmente importante é o modus operandi dos atacantes: publicam uma aplicação totalmente fiável nos respectivos mercados, mantêm-na um par de dias para obter qualificações positivas e ganhar a confiança dos utilizadores, e depois mudam a APK para um serviço trojanizado com o objectivo de cumprir com os seus fins maliciosos", explica Catalin Cosoi, Responsável de Ameaças Online do Laboratório da Bitdefender, que adiciona: "É também de grande importância que

a maioria das aplicações de repacking que analisamos têm baixas taxas de detecção, o que representa um perigo real, inclusive para os utilizadores de smartphones que possuem uma solução de segurança móvel".

Android.Trojan.FakeUpdates.A apresenta uma ameaça imediata para o utilizador do smartphone, já que pode descarregar e instalar qualquer coisa, desde versões de teste que depois pedem um pagamento para se instalarem totalmente, spyware e trojans.

Para proteger a privacidade e manter o dispositivo seguro, a Bitdefender aconselha a não instalar aplicações que solicitem mais permissões do que as que normalmente são necessárias para que uma aplicação funcione. Para além do mais, a instalação de uma solução de segurança móvel ajudará a mitigar este tipo de ataques.

Para mais informações sobre a actualidade informática siga Bitdefender Portugal no [Facebook](#) e no .

Inscreva-se para aceder ao apoio técnico e outros serviços personalizados do BitDefender. Se já tem uma conta, por favor [inicie sessão](#).

Os utilizadores registados do BitDefender beneficiam de ofertas especiais de actualizações, descontos nas renovações das licenças, acesso a versões beta fechadas do software BitDefender, apoio técnico prioritário gratuito 24x7.

O registo é um processo com três passos:

1. introduza um endereço electrónico válido e os dados pessoais e clique em **Seguinte**
2. introduza a chave de licença que adquiriu e clique em **Seguinte**
3. Siga as instruções da mensagem electrónica de confirmação.

Importante: Introduza um endereço electrónico **válido**. Será enviada uma mensagem electrónica para o endereço que indicar. O seu registo não poderá ser concluído se não receber a mensagem de confirmação.