Loja do Google tinha 500 apps infectados com mais de 100 milhões de downloads[1]

Gustavo Sumares 22/08/2017 11h34 Android Aplicativos Google Play

A empresa de segurança digital Lookout detectou uma falha presente em mais de 500 aplicativos disponíveis para download na Play Store, a loja oficial de apps do Google. No total, os aplicativos afetados já tinham sido baixado mais de 100 milhões de vezes.

De acordo com a empresa, os aplicativos estavam na loja porque a falha de segurança não se encontrava diretamente no código deles. Os desenvolvedores dos apps provavelmente sequer tinham consciência do risco que suas criações apresentavam. Isso porque os apps afetados usavam uma ferramenta de desenvolvimento de software chamada Igenix que, ela sim, era responsável pela brecha.

O Igenix é um sistema que facilita a comunicação dos aplicativos com redes de propagandas. O que ele fazia era coletar algumas informações dos usuários para, com base nelas, direcionar propagandas mais adequadas aos gostos dele. No entanto, de acordo com a Lookout, os dados coletados pelo sistema iam além do que ele tinha permissão para fazer.

Instala primeiro, infecta depois

Conforme a empresa de segurança explica, o aplicativo que ficava na Play Store não tinha, de fato, nenhuma vulnerabilidade. No entanto, quando ele era instalado, ele fazia uma requisição a um servidor controlado pela Igenix e, por meio dele, fazia o download de grandes arquivos criptografados que, eles sim, continham código malicioso.

Eles permitiam, de acordo com o ArsTechnica que o aplicativo coletasse dados como os registros de chamadas do usuário, incluindo os números que ligaram para aquele celular, os números para os quais ele ligou e o horário das chamadas. Outros dados roubados pelo sistema eram a lista de locais do GPS do celular, a lista de redes Wi-Fi próximas e a lista de aplicativos instalados. Com esses dados, o sistema conseguia rastrear de maneira extremamente invasiva a navegação das vítimas.

Apps afetados

Segundo a empresa de segurança, o Igenix "é relativamente original porque os desenvolvedores não estão criando a funcionalidade maliciosa - nem têm controle sobre quais atividades maliciosas o app pode vir a executar." A lista de aplicativos infectados incluía jogos voltado para adolescentes, ao menos um dos quais foi baixado entre 50 milhões e 100 milhões de vezes.

Fora eles, estavam infectados também aplicativos de clima e meteorologia (um dos quais tinha entre um milhão e 5 milhões de downloads), editores de imagem (um dos quais tinha esse mesmo número) e apps de rádio pela internet (um dos quais tinha entre 500 mil e um milhão de downloads). Apps educativos, de saúde, de viagem e de emojis também foram afetados, mas em escala menor.

---

[1] https://olhardigital.com.br/fique_seguro/noticia/loja-do-google-tinha-500-apps-infectados-com-mais-de-100-milhoes-de-downloads/70554

Resposta

Um representante do Google entrou em contato com o ArsTechnica dizendo que a empresa já "tomou ações" quanto a esses aplicativos, e que eles já "asseguraram versões anteriores dos apps já baixadas". Dessa maneira, as funções maliciosas incorporadas aos aplicativos por meio dos servidores da Igenix não deve estar mais ativa.

Vale notar que nem todos os 500 apps detectados pela Lookout tinham, de fato, funções maliciosas. No entanto, como eles usavam o sistema da Igenix, essas funções poderiam ser baixadas por eles a qualquer momento por meio de uma atualização. A recomendação da empresa para evitar ameaças desse tipo é utilizar uma solução de antivírus no celular.

Outra coisa importante é esperar um tempo para fazer download. Atualizar sistema deve ser feito, mas outros aplicativos, que foi o caso, podem esperar, principalmente se você já tem a versão anterior.