rastreamento do software pré-instalado neste ecossistema

JORDI PÉREZ COLOMÉ

Madri - 19 MAR 2019 - 14:54 BRT

Juan Tapiador (esquerda) e Narseo Vallina-Rodríguez, chefes da pesquisa sobre o software pré-instalado nos celulares Android. KIKE PARA

Um usuário compra um celular Android novo. Tanto faz a marca. Abre a caixa, aperta o botão de ligar, o celular se conecta à Internet e, sem fazer nada mais, ele acaba de iniciar a mais sofisticada máquina de vigilância da sua rotina.

Não importa se você vai baixar o Facebook, ativar sua conta do Google ou dar todas as permissões de acesso a qualquer aplicativo esquisito de lanterna ou antivírus. Antes de executar qualquer ação, seu celular novo já começou a compartilhar detalhes da sua vida. O software pré-instalado de fábrica é o recurso mais perfeito desse celular para saber sua atividade futura: onde está, o que ele baixa, quais mensagens manda, que arquivos de música guarda.

"Os aplicativos pré-instalados são a manifestação de outro fenômeno: acordos entre atores (fabricantes, comerciantes de dados, operadoras, anunciantes) para, em princípio, agregar valor, mas também para fins comerciais. O elemento mais grave nisso é a escala: falamos de centenas de milhões ou de bilhões de telefones Android", diz Juan Tapiador, professor da Universidade Carlos III e um dos autores, junto com Narseo Vallina-Rodríguez, do IMDEA Networks e do ICSI (Universidade de Berkeley), da investigação que revela esse submundo. Os celulares Android representam mais de 80% do mercado global.

> ***O elemento mais grave nisso é a escala: falamos de centenas de milhões ou de bilhões de telefones Android***
>
> ”

Juan Tapiador, professor

O novo estudo comandado pelos dois acadêmicos espanhóis revela a profundidade do abismo. Nenhuma das conclusões é radicalmente nova por si só: já se sabia que os celulares andam no limite das autorizações de uso na hora de colher e compartilhar dados. A novidade da função dos aplicativos pré-instalados está em sua extensão, falta de transparência e posição privilegiada dentro do celular: foram analisados 1.742 celulares de 214 fabricantes em 130 países.

"Até agora as pesquisas sobre os riscos de privacidade em celulares se centravam em aplicativos que estão listados no Google Play ou em amostras de *malware*", diz Vallina. Desta vez, foram analisados os softwares que os celulares trazem de série, e a situação parece fora de controle. Devido à complexidade do ecossistema, as garantias de privacidade da plataforma Android podem estar em xeque.

O artigo, que será publicado oficialmente em 1º de abril e ao qual o EL PAÍS teve acesso, já foi aceito por uma das principais conferências de segurança cibernética e privacidade do mundo, o IEEE Symposium on Security & Privacy, da Califórnia.

Nossa informação pessoal é enviada a uma ampla rede de destinos, que muda segundo o celular, e alguns são polêmicos: para servidores do fabricante do celular, para empresas habitualmente acusadas de espionar nossas vidas —Facebook, Google— e para um obscuro mundo que vai de corporações a *start-ups* que reúnem a informação pessoal de cada um, empacotam-na com um identificador vinculado ao nosso nome e a vendem a quem pagar bem.

> **Nossa informação pessoal é enviada a uma ampla rede de destinos, alguns deles polêmicos**

Ninguém até agora havia se debruçado sobre este abismo para fazer uma investigação dessa magnitude. Os pesquisadores criaram o aplicativo Firmware Scanner, que recolhia o software pré-instalado dos usuários voluntários que o baixavam. Mais de 1.700 aparelhos foram analisados nesse estudo, mas o aplicativo está instalado em mais de 8.000. O código aberto do sistema operacional Android permite que qualquer fabricante tenha sua versão, junto com seus *apps* pré-instalados. Um celular pode ter mais de 100 aplicativos pré-instalados e outras centenas de bibliotecas, que são serviços de terceiros

incluídos em seu código, muitos deles especializados em vigilância do usuário e publicidade.

Ao todo, um panorama internacional de centenas de milhares de aplicativos com funções comuns, duvidosas, desconhecidas, perigosas ou potencialmente delitivas. Essa quase perfeita definição do termo caos levou os pesquisadores a mais de um ano de exploração. O resultado é só um primeiro olhar para o precipício da vigilância maciça de nossos celulares Android sem conhecimento do usuário.

Mais de um fabricante

Um celular Android não é produto apenas do seu fabricante. A afirmação é surpreendente, mas na cadeia de produção participam várias empresas: o chip é de uma marca, as atualizações do sistema operacional podem estar terceirizadas, as operadoras de telefonia e as grandes redes de varejo que vendem celulares acrescentam seu próprio software. Os atores que participam da fabricação de um celular vão muito além do nome que aparece na caixa. É impossível determinar o controle definitivo de todo o software lá colocado, e quem tem acesso privilegiado aos dados do usuário.

O resultado é um ecossistema descontrolado, onde atualmente ninguém é capaz de assumir a responsabilidade do que ocorre com nossa informação mais íntima. O Google criou a plataforma a partir de código livre, mas agora ele é de todos. E o que é de todos não é de ninguém: "O mundo Android é muito selvagem, é como um faroeste, especialmente em países com escassa regulação de proteção de dados pessoais", diz Tapiador.

"Não há nenhum tipo de supervisão sobre o que se importa e comercializa em termos de software (e em grande medida de hardware) dentro da União Europeia", diz Vallina. O resultado? Um caos, onde cada versão de nossos celulares Android conversa com sua base desde o primeiro dia, sem interrupção, para lhe contar o que fazemos. O problema não é só o que contam sobre nós, mas que o dono do celular não controle a quem dá permissões.

O jardim fechado do Google Play

As empresas que reúnem dados de usuários para, por exemplo, criar perfis para anunciantes já têm acesso aos dados do usuário através dos aplicativos normais do Google Play. Então que interesse um comerciante de dados tem em chegar a acordos com fabricantes para participar do software pré-instalado?

Imaginemos que nossos dados estão dentro de uma casa de vários andares. Os aplicativos do Google Play são janelas que abrimos e fechamos: às vezes deixamos os dados sair, e às vezes não. Depende da vigilância de cada usuário e das autorizações concedidas. Mas o que esse usuário não sabe é que os celulares Android vêm com a porta da rua escancarada. Tanto faz o que você fizer com as janelas.

O software pré-instalado está sempre lá, acompanha o celular para cima e para baixo, e além do mais não pode ser apagado sem rootear o dispositivo – romper a proteção oferecida do sistema para fazer o que quiser com ele, algo que não está ao alcance de usuários comuns.

> **Esse usuário não sabe que os celulares Android vêm com a porta da rua escancarada**

Os aplicativos que o usuário baixa do Google Play dão a opção de ver as permissões concedidas: autoriza seu novo jogo gratuito a acessar seu microfone? Permite que seu novo *app* acesse a sua localização para ter melhor produtividade? Se nos parecerem permissões demais, podemos cancelá-las. Os aplicativos que o Google fiscaliza têm seus termos de serviço e devem pedir uma autorização explícita para executar ações.

O usuário, embora não repare ou não tenha outro remédio, é o responsável final por suas decisões. Ele está autorizando alguém a acessar seus contatos. Mas os aplicativos pré-instaladas já estão lá. Vivem por baixo dos aplicativos indexados na loja, sem permissões claras ou, em muitos casos, com as mesmas permissões que o sistema operacional – quer dizer, todas. "O Google Play é um jardim fechado com seus policiais, mas 91% dos aplicativos pré-instalados que vimos não estão no Google Play", diz Tapiador. Fora do Google Play ninguém vigia em detalhe o que acaba dentro de um celular.

Dois problemas agregados

O software pré-instalado tem outros dois problemas agregados: fica junto do sistema operacional, que tem acesso a todas as funções de um celular, e, dois, esses aplicativos podem ser atualizados e podem mudar.

O sistema operacional é o cérebro do celular. Sempre tem acesso a tudo. Independe que o aplicativo esteja acionado ou que o usuário possa apagá-la. Estará sempre lá e, além disso, é atualizado. Por que as atualizações são importantes? Aqui vai um exemplo: um fabricante autorizou uma empresa a colocar no celular um código que comprove algo inócuo. Mas esse código pode ser atualizado e, dois meses depois, ou quando a empresa souber que o usuário vive em tal país e trabalha em tal lugar, mandar uma atualização para fazer outras coisas. Quais? Qualquer coisa: gravar conversas, tirar fotos, olhar mensagens...

Os aplicativos pré-instaladas são fáceis de atualizar por seu criador: se muda o país ou as intenções de quem colocou lá um sistema de rastreamento, manda-se um novo software com novas ordens. O proprietário de seu celular não pode impedi-lo e nem sequer lhe pedem permissões específicas: atualiza-se o seu sistema operacional.

> ***Essa informação às vezes é descomunal: características técnicas do telefone, identificadores únicos, localização, contatos, mensagens e e-mails***
>
> **JUAN TAPIADOR, PROFESSOR**

"Alguns desses aplicativos *ligam para casa* pedindo instruções e mandam informação sobre onde estão instalados. Essa informação às vezes é descomunal: relatórios extensos com características técnicas do telefone, identificadores únicos, localização, contatos na agenda, mensagens e e-mails. Tudo isso é reunido num servidor, e é tomada uma decisão sobre o que fazer com esse celular. Por exemplo, segundo o país no qual se encontre, o software pode decidir instalar um ou outro aplicativo, ou promover determinados anúncios. Verificamos isso analisando o código e o comportamento dos aplicativos", diz Tapiador.

O servidor que recebe a informação inclui desde o fabricante, uma rede social que vende publicidade, um desconhecido comerciante de dados ou um obscuro endereço IP que ninguém sabe a quem pertence.

Um perigo é que esses obscuros aplicativos pré-instalados usam as permissões personalizadas (*custom permissions*) para expor informação a aplicativos da Play Store. As permissões personalizadas são uma ferramenta que o Android oferece aos desenvolvedores de software para que os aplicativos compartilhem dados entre si. Por exemplo, se um operador ou um serviço de banco tem várias, é plausível que possam falar entre si e compartilhar dados. Mas às vezes não é simples verificar quais dados algumas peças desse software compartilham.

Dentro de um celular novo há por exemplo um aplicativo pré-instalado que tem acesso a câmera, aos contatos e ao microfone. Esse aplicativo foi programado por um sujeito chamado Wang Sánchez e tem um certificado com sua chave pública e sua assinatura. Aparentemente é legítima, mas ninguém comprova que o certificado de Wang Sánchez seja real. Esse aplicativo está sempre ligado, capta a localização, ativa o microfone e conserva as gravações. Mas não manda isso a nenhum servidor, porque o aplicativo de Wang Sánchez não tem permissão para enviar nada pela Internet. O que ele faz é declarar uma permissão personalizada que regula o acesso a esses dados: quem tiver essa permissão poderá obtê-los.

Aí um dia o proprietário desse celular vai à Google Play Store e encontra um aplicativo esportivo magnífico. Que permissões oficiais lhe pedem? Só acessar a Internet, o que é perfeitamente comum entre aplicativos. E também pede a permissão personalizada do aplicativo de Wang Sánchez. Mas você não percebe, porque estas permissões não são mostradas ao usuário. Então, a primeira coisa que o *app* esportivo recém-chegado dirá ao pré-instalado é: "Ah, você mora aqui? Me dá acesso ao microfone e à câmera?". Era aparentemente um *app* sem risco, mas as complexidades do sistema de permissões tornam possíveis situações desse tipo.

Os Governos e a indústria há anos conhecem esse emaranhado. As agências federais dos Estados Unidos pedem seus celulares com sistemas operacionais livres deste software pré-instalado e adaptados às suas necessidades. E os cidadãos? Que se virem. Seus dados não são tão secretos como os de um ministério.

"Exercer controle regulatório sobre todas as versões possíveis do Android do mercado é quase impraticável. Exigiria uma análise muito extensa e custosa", explica Vallina. Esse caos lá fora permite que sofisticadas máquinas de vigilância maciça vivam em nossos bolsos.

OS AUTORES DOS APLICATIVOS

Os autores desses aplicativos são um dos grandes mistérios do Android. A investigação encontrou um panorama similar ao submundo da *Dark Web*: há, por exemplo, aplicativos assinados por alguém que diz ser "o Google", mas não tem jeito de sê-lo. "A atribuição aos atores foi feita quase manualmente em função do vendedor no qual se encontram, quem as assina e se têm, por exemplo, alguma cadeia que identifique alguma biblioteca ou fabricante conhecido", diz Vallina. O resultado é que há muitas que mandam informação aceitável a fabricantes ou grandes empresas, mas muitas outras se escondem detrás de nomes enganosos ou falsos.

Essa informação é facilmente vinculada a um número de telefone ou dados pessoais como nomes e sobrenomes, não a números identificativos tratados de forma anônima. O telefone sabe quem é o seu dono. O chip e dúzias de aplicativos vinculados ao e-mail ou à sua conta em redes sociais revelam facilmente a origem dos dados.

ARQUIVADO EM:

Android · Google · Celulares · Motores pesquisa · Alphabet · Sistemas operacionais · Telefonia celular multimídia · Privacidade internet · Programas informáticos · Celular · Segurança internet · Informática · Mobilidade · Telefonia · Internet · Empresas · Tecnologia