Norton by Symantec

O BOM, O MAU E O SORRATEIRO. VOCÊ ESTÁ CIENTE DO QUE SEUS APLICATIVOS ESTÃO FAZENDO?

Os aplicativos podem ser divertidos, produtivos e gratuitos, mas também podem atacar com custos ocultos e mau comportamento. Pare de responder aos riscos e passe a adotar uma nova abordagem proativa para a proteção de seus dispositivos móveis.

Sumário

Os dispositivos móveis inteligentes estão hoje em todo lugar. Globalmente, quase 1,8 bilhões de pessoas ou um quarto da população mundial têm um smartphone.[1] À medida que o uso dos dispositivos móveis aumenta, também aumenta o uso dos aplicativos.

Os usuários de smartphones em todo o mundo passam 86% de seu tempo usando aplicativos e apenas 14% na Internet.[2] Globalmente, o número médio de aplicativos instalados é de 26 por aparelho e, entre os 10 principais países, essa média sobe para mais de 35.[3]

Os aplicativos promovem a liberdade, uma vez que permitem que você faça em seu dispositivo móvel tudo o que pode fazer no PC, inclusive de maneiras novas e diferentes, conforme utilizamos mais a Internet. Por exemplo, você já pode usar os aplicativos para controlar a temperatura da sala de sua casa, acender as luzes antes de chegar em casa e manter a casa protegida contra ladrões.

Os aplicativos fazem tudo acontecer. Se o telefone fosse um veículo, os aplicativos seriam o volante, o acelerador e o pisca-pisca. Eles também são a chave que abre a porta para todas as informações que o dispositivo móvel contém e todas as informações que você armazena na nuvem.

Os criminosos estão atentos. Suas informações pessoais valem dinheiro, e os hackers estão cada vez mais usando táticas testadas e comprovadas (como aplicativos falsos e ransomware) para atacar dispositivos móveis. E eles não são os únicos. Desenvolvedores de aplicativos gananciosos também estão atrás de suas informações pessoais. Seus objetivos não são necessariamente ilegais. Eles podem estar simplesmente tentando inserir anúncios direcionados em sua barra de notificação. Porém seus métodos podem apresentar riscos.

Considerando que há tantos interessados em suas informações confidenciais, é mais importante do que nunca que você saiba o que seus aplicativos estão fazendo e tome medidas para manter seus dispositivos móveis sempre seguros.

A simples localização e bloqueio de um celular perdido hoje já não é suficiente. Sim, essas medidas de proteção reativas são proteções importantes. Mas a nova diretriz é segurança proativa. Isso quer dizer não só proteção total contra aplicativos maliciosos que roubam dinheiro e dados pessoais, mas também proteção que o capacita a tomar decisões informadas sobre os riscos potenciais dos aplicativos baixados. E, é claro, se esses aplicativos gratuitos valem mesmo a pena.

A proteção de dispositivos móveis agora demanda uma abordagem nova e preventiva, para que você possa desfrutar de todos os benefícios do nosso universo de aplicativos.

[1] eMarketer: http://www.emarketer.com/Article/Worldwide-Smartphone-Usage-Grow-25-2014/1010920
[2] Flurry: http://www.flurry.com/bid/109749/Apps-Solidify-Leadership-Six-Years-into-the-Mobile-Revolution#.VH5uBmctDIU
[3] Our Mobile Planet: http://think.withgoogle.com/mobileplanet/en/

Você está ciente do que seus aplicativos estão fazendo? O Norton está.

Muitos clientes tendem a considerar os aplicativos para dispositivos móveis com a mesma ingenuidade que consideravam o software para desktops há 10 ou 15 anos atrás. Eles instalam aplicativos para dispositivos móveis sem pouca ou nenhuma consideração dos riscos que eles podem representar, e instalam muitos desses aplicativos, porque o seu download é feito com um único clique.

Os aplicativos (principalmente os gratuitos) sempre informam os benefícios que oferecem, mas não seus "custos" reais. Esses custos podem ser ameaças ocultas ou outros riscos potenciais. A área restrita dos sistemas operacionais iOS da Apple, combinada a seus rigorosos controles do que entra em sua app store do iTunes, dificulta a ocorrência de aplicativos maliciosos. A natureza aberta do sistema operacional Android, porém, pode ser mais facilmente manipulada para causar ameaças e riscos potenciais.

O Relatório Symantec de Ameaças à Segurança na Internet revelou que o malware para dispositivos móveis em 2013 foi desenvolvido quase que exclusivamente para o sistema operacional Android, com 32% desses aplicativos roubando as informações pessoais do usuário.[4]

Além disso, mais de 75% de todos os aplicativos para dispositivos móveis falharam nos testes de segurança básicos, executando uma variedade de comportamentos maliciosos arriscados.[5]

A Symantec registrou um aumento de 69% em instâncias de malware de dispositivos móveis entre 2012 e 2013.

[4] Relatório Symantec de Ameaças à Segurança na Internet, 2014: http://www.symantec.com/security_response/publications/threatreport.jsp
[5] Gartner: http://www.gartner.com/newsroom/id/2846017

Norton by Symantec

Os aplicativos maliciosos são maliciosos

É fácil de entender porque os aplicativos para dispositivos móveis atraem os hackers. A base de usuários tem aumentado rapidamente e o volume de informações que pode ser obtido com o uso do aplicativo malicioso é significativo. Os hackers, como era de se esperar, estão cada vez melhores. Eles estão aprendendo e compartilhando mais, e seus ataques se tornam cada vez mais sofisticados. Os criminosos cibernéticos estão aplicando suas táticas para PCs (como phishing, software falso e ransomware) nos dispositivos móveis.

Em um único golpe de aplicativo falso, os phishers ofereceram um aplicativo que prometia minutos gratuitos em chamadas de celulares. Essa oferta estaria disponível somente se o usuário inserisse suas credenciais de login e encaminhasse a oferta para 10 amigos. O golpe tinha como objetivo aumentar o número de vítimas, roubando credenciais e coletando outros dados pessoais.

Outro aplicativo falso copiou o aplicativo verdadeiro do Mizrahi Bank, um dos maiores bancos de Israel. Os hackers incluíram esse aplicativo na loja do Google Play e, sem suspeitar de nada, os clientes do banco fizeram o download. Quando eles abriram o aplicativo e inseriram suas informações de login, o aplicativo roubou as IDs de usuário. O aplicativo enviou uma mensagem de erro instruindo os clientes a reinstalar o aplicativo real do banco, que então funcionou normalmente. A maioria dos clientes nem suspeitou que suas IDs de usuário foram roubados.

Outra ameaça recente foi o Android. Simplocker, um Cavalo de Troia de ransomware, fornecido por um aplicativo falso. Uma vez instalado em seu dispositivo, ele criptografa (ou bloqueia) os arquivos e depois exibe um alerta falso do FBI, afirmando que foi encontrado conteúdo pornográfico ilegal em seu dispositivo. Você é instruído a pagar US$300 de "multa" através de um serviço de pagamento chamado MoneyPack para desbloquear seus arquivos.

Guia rápido de aplicativos maliciosos

Mais de 20% dos 15 milhões de aplicativos analisados até hoje pelo Norton são maliciosos. Eles apresentam uma variedade de formatos:

Aplicativos de rastreamento coletam mensagens de texto e logs de chamadas, rastreiam coordenadas do GPS, gravam chamadas e roubam fotos e vídeos dos dispositivos. O relatório Norton de 2014 mostrou que o volume das ameaças de rastreamento de usuários em 2013 aumento de 15 para 30%.

Aplicativos para roubo coleta dados específicos de usuários e dispositivos, como informações do dispositivo, dados da configuração e conteúdo pessoal.

Aplicativos para infecção executam funções de malware tradicional, como a instalação de aplicativos de porta dos fundos e carregadores que concedem aos hackers acesso a seu dispositivo.

Aplicativos de reconfiguração elevam os privilégios ou modificam as configurações no sistema operacional, o que pode abrir as portas para os agressores.

Aplicativos para roubo de dinheiro utilizam números de mensagens de texto com código curto e tarifa premium. Os hackers criam um malware que envia mensagens de texto a esses números a partir de dispositivos infectados. Os usuários recebem uma conta de seu provedor e o hacker recebe o dinheiro.

Aplicativos para roubos de dois fatores podem interceptar uma mensagem de texto de seu banco, que contenha um código de autenticação único, o que pode dar aos hackers acesso a sua conta bancária.

O grayware também pode ser arriscado

A diferença entre o software legítimo e o malware não é muito clara. Uma certa categoria de aplicativos chamada *grayware* ocupa esse local intermediário. Nesse ínterim, encontram-se vários desenvolvedores não maliciosos que acham mais fácil convencer os usuários a fazer o download de aplicativos potencialmente arriscados, que expõem informações e conteúdo, muitas vezes usando um aplicativo "gratuito" como isca.

Os aplicativos grayware não contêm códigos maliciosos, mas podem comprometer sua privacidade e afetar seu dispositivo com anúncios e vários tipos de comportamentos inconvenientes. Um tipo comum de grayware, chamado *mobile adware* ou *madware*, são os aplicativos que exibem anúncios em uma barra de notificação do telefone, substituem o tom de discagem por anúncios falados ou, ainda pior, expõem dados privados, como números de telefones e informações da conta do usuário.

Se você tiver um alto grau de conhecimento técnico e se propor a ler cuidadosamente a longa lista de permissões dos aplicativos com a qual concordou ao fazer o download do app no Google Play, talvez consiga detectar vários desses riscos. Porém, esse nem sempre é o caso. Mesmo que leia os aceites, você não conhecerá todos os comportamentos reais do aplicativo.

A pesquisa do Norton mostra que mais de

60%

dos aplicativos para Android contêm adware ou outro grayware.

Após instalado, o grayware poderá rastrear sua localização ou monitorar sua navegação na Internet, e até vender essas informações no mercado. Muitas vezes o aplicativo tem uma justificativa razoável para coletar dados confidenciais. Porém, normalmente você não tem ciência desse comportamento e provavelmente não se sente seguro compartilhando certas informações com esse aplicativo. Por exemplo, um aplicativo que coleta o número de seu telefone como ID exclusivo de seu dispositivo e o envia através da rede, sem criptografia. Repentinamente, o número de seu telefone fica facilmente disponível a golpistas e hackers.

Ou um aplicativo pode apresentar um risco potencial à privacidade quando coleta informações incoerentes com sua finalidade. Por exemplo, por que um aplicativo de previsão de tempo precisa acessar seus contatos ou as informações de seu calendário?

Igualmente comuns são os aplicativos que esgotam a bateria do aparelho, comprometem seu desempenho ou consomem dados através da rede aumentando consideravelmente a conta do aparelho. Tecnicamente esses aplicativos não são grayware, mas com certeza são inconvenientes. Muitos deles são executados secretamente em segundo plano. Você nota que a bateria de seu dispositivo reduz à medida que tempo passa desde que você o adquiriu? Os aplicativos podem ser a causa disso. As tarifas de seu plano de dados ficaram inesperadamente altas? Novamente, os aplicativos. Muitos fazem vários downloads, mesmo quando não estão abertos.

O Norton oferece proteção líder para os dispositivos móveis

Você confia em ter o Norton no PC. Aplicamos a mesma tecnologia de ponta, recursos para pesquisa profunda e recursos de inteligência global para proteger seus dispositivos móveis.

A maioria dos produtos para a segurança de dispositivos móveis atuais fornecem proteção básica. Fazer um esforço extra para proporcionar uma tecnologia que o proteja totalmente contra aplicativos maliciosos e inconvenientes. Utilizamos nossos 30 anos de expertise em segurança e o maior banco de dados de ameaças do mundo para mantê-lo seguro contra as ameaças aos aplicativos para Android.

O Norton Mobile Insight nunca dorme

Todos os dados dos aplicativos Android que coletamos através do Norton Mobile Insight, examinando constantemente mais de 200 app stores e compilando informações da rede Norton Community Watch, são inseridos em nossa pipeline de processamento e executados através de um conjunto robusto de ferramentas que identificam aqueles que representam problemas.

Primeiro executamos uma análise estática, que inclui a extração de dados básicos como o título do aplicativo, a assinatura do desenvolvedor e a lista de permissões, que normalmente está presente no download do app, e pode ser extremamente longa.

Em seguida, aprofundamos ainda mais no código do aplicativo a fim de descobrir quais interfaces de programa de aplicativo (API) confidenciais serão solicitadas. Por exemplo, o aplicativo está solicitando APIs para ler números de telefone e outras informações privadas e depois acessar a Internet? E a investigação não para por aqui. Descobrimos se o aplicativo é localizado. Ele é instalado sem a inserção de um ícone no iniciador? Essas informações fornecem dicas importantes sobre a segurança do aplicativo.

Em seguida, executamos uma análise dinâmica importante, que fornece uma visão sem precedentes da privacidade do aplicativo e do vazamento das informações. Executamos todos os aplicativos através de um emulador Android instrumentado, para que o aplicativo pense que está sendo executado no mundo real. Por exemplo, se um aplicativo coleta e envia informações pessoais ou do dispositivo para fora do dispositivo em segundo plano, essas informações podem estar indo para o site de um fornecedor indesejado.

Fazemos essa análise de forma inteligente e automatizada, exercitando os fluxos de uso e recursos reais. Muitos de nossos concorrentes simplesmente deduzem os comportamentos dos aplicativos para dispositivos móveis e relatam os riscos com base nas permissões do aplicativo, sem fazer nenhum teste real, o que pode resultar no relato de informações imprecisas ou alarmes falsos para o usuário.

Nossas tecnologias e recursos da informação exclusivos incluem:

O Norton™ Mobile Insight é um sistema dinâmico que constantemente faz o download e analisa novos aplicativos para Android de mais de 200 app stores, incluindo Google Play, gerando uma inteligência de aplicativos exclusiva e permanente. Analisamos mais de 30.000 aplicativos novos todos os dias e mais de 15 milhões de aplicativos até hoje.

O Norton Community Watch é uma comunidade movimentada, que consiste em milhões de usuários e nos permite coletar metadados anônimos e metadados de desempenho de outros aplicativos executados nos dispositivos Android, incluindo vários arquivos de aplicativos nunca vistos. A utilização desses dados da comunidade e a execução de uma análise em tempo real concedem ao Norton Mobile Insight outra forma de entender o comportamento de um aplicativo depois de instalado, além dos riscos envolvidos em mantê-lo no dispositivo. Na verdade, 25% dos aplicativos conhecidos analisados pelo Norton Mobile Insight são coletados somente no Norton Community Watch, o que significa que estamos analisando e aprendendo sobre muitos aplicativos não distribuídos através das app stores.

A divisão da STAR (Symantec Security Technology and Response) é formada por uma equipe global de engenheiros de segurança, caçadores de vírus, analistas de ameaças e pesquisadores que proporcionam a tecnologia de segurança, conteúdo e suporte básicos para todos os produtos da Symantec, incluindo os de dispositivos móveis. Esses especialistas representam nossos olhos e ouvidos, pesquisando o cenário de ameaças dia e noite para manter sua segurança.

Dados: quanto mais você tiver, mais conhecimento terá

E, finalmente, a solução Norton promove o importante Symantec Data Analytics Platform (SDAP), um dos raros sistemas poderosos e ágeis o suficiente para se manter à frente do enorme crescimento das ameaças cibernéticas e do uso de dispositivos móveis.

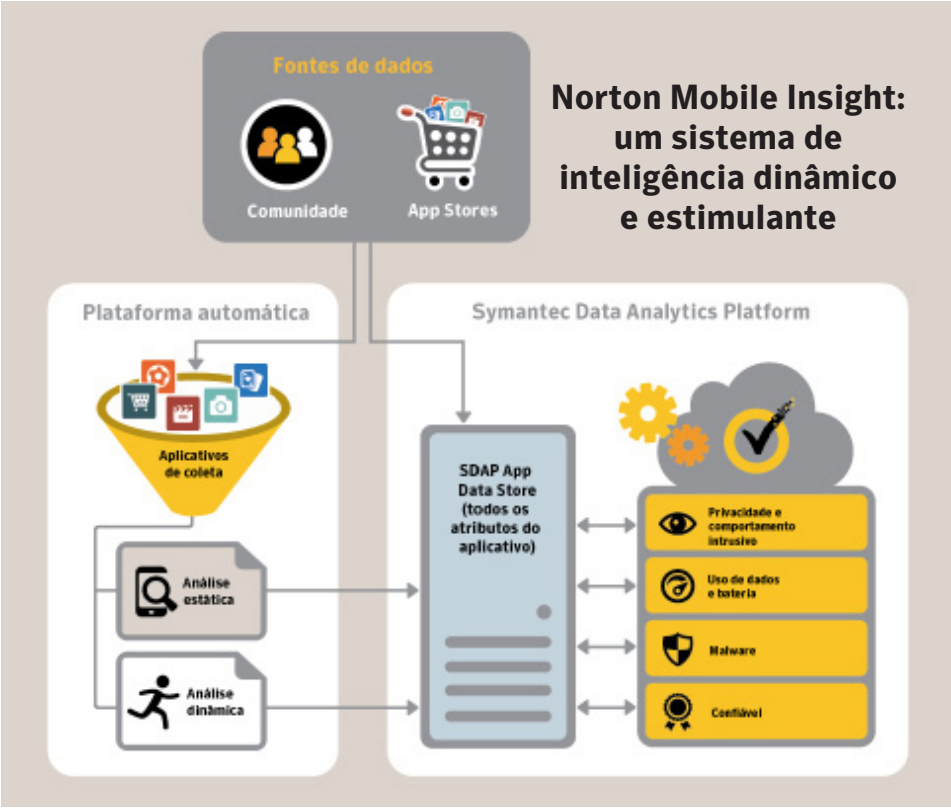
A plataforma SDAP é um enorme banco de dados, sempre em expansão, que abriga todos os nossos dados de segurança. Nossos dados de dispositivos móveis incluem aproximadamente 1,6 trilhões de partes de dados individuais. Esse número é bastante significativo. É o que é necessário para proteger seu dispositivo contra as ameaças aos dispositivos móveis.

Todos os dados de aplicativos que coletamos, desde comportamentos do aplicativo até sua estabilidade e detalhes do desempenho, são processados pela plataforma SDAP. Esses dados incluem informações sobre o desempenho do aplicativo no mundo real, quantas pessoas no Norton Community Watch já o utilizaram, em quais app stores ele se encontra e quantas pessoas já fizeram o seu download.

Analisamos todos os dados para então determinar se o aplicativo é malicioso ou não. O Norton Mobile Insight já processou mais de 15 milhões de aplicativos até hoje e processa 30.000 novos aplicativos todos os dias. Ele detecta os recursos e modelos que significam malware, verifica aplicativos em busca de comportamentos intrusivos e suspeitos, além de examinar o uso de dados e da bateria.

E está cada vez mais inteligente, à medida que o cenário de ameaças se transforma. Ele aprende e evolui com base nos novos dados que ele coleta. Por exemplo, ele sabe que o tamanho do aplicativo no malware tende a ser menor do que em aplicativos não maliciosos, pois os desenvolvedores de malware normalmente não gastam tempo no refinamento de suas criações.

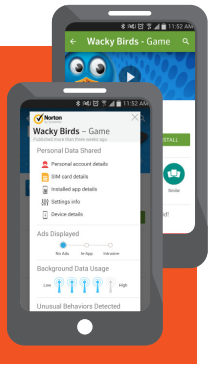
O Norton Mobile Insight então correlaciona todas essas informações com centenas de outros pontos de dados para verificar se o aplicativo é malware e define um nível de confiança para a segurança do aplicativo. Ele reconhece elementos inerentes ao malware que um agressor não consegue alterar facilmente, como modelos de códigos, técnicas para a execução de comportamentos maliciosos e o status da reputação do desenvolvedor na comunidade.



Uma proteção avançada e proativa é necessária no atual universo de aplicativos

O Norton Mobile Security é uma assinatura de produto baseada na Web, criada para proteger você e seus dispositivos móveis. Ele é ativado pela poderosa tecnologia Norton Mobile Insight discutida neste documento. O Norton Mobile Security foi criado para economizar tempo e eliminar o elemento "adivinhação" da identificação de aplicativos com todos os riscos aqui discutidos.

A chave para o Norton Mobile Security é um recurso de verificação de aplicativo chamado App Advisor.



Com a tecnologia Norton Mobile Insight, o App Advisor fornece proteção proativa, permitindo que você verifique aplicativos automaticamente no Google Play ANTES de fazer o download (no Android 4.0 ou posterior, Android 4.2 ou posterior e dispositivos Samsung). Ele informa se os aplicativos contêm códigos maliciosos ou se apresentam riscos à privacidade, comportamento intrusivo ou alto uso de dados ou da bateria. Ele verifica também automaticamente os aplicativos para Android baixados anteriormente ou aplicativos instalados fora de uma app store, em busca dos mesmos riscos, permitindo que você remova os aplicativos, se desejar.

Em uma única e simples medida, você pode facilmente tomar decisões informadas sobre os aplicativos Android. Você pode decidir quando vale a pena obter determinado aplicativo.

O Norton Mobile Security também fornece componentes de proteção proativa para você e seus dispositivos Android, com Proteção para a Web, que o mantém protegido contra sites fraudulentos criados para roubar suas informações pessoais e seu dinheiro. Ele inclui também proteção para a recuperação remota de dispositivos para Android, iPhone e iPad, para que você possa localizá-los rapidamente. Você pode até mesmo salvar suas informações de contato e restaurá-las no caso de perda ou roubo. Agora ficou fácil proteger todos os seus dispositivos com um único serviço de assinatura baseado na Web. O Norton Mobile Security deixa que você explore todo o potencial da praticidade e liberdade dos dispositivos móveis, de forma segura.

Ouse com a solução do Norton

A mobilidade é essencial para sua vida movimentada e conectada. Porém, nossa dependência cada vez maior desses pequenos computadores (os dispositivos móveis) torna essencial reconhecer os riscos à segurança de dispositivos móveis e tomar medidas de proteção.

Oferecemos também as tecnologias de proteção do Norton Mobile, como parte da assinatura de produtos de nossas variadas plataformas Norton Security, Norton Security com Backup e Norton Small Business. Essas três assinaturas fornecem a você, sua família e sua empresa uma proteção personalizada para PCs, Macs e dispositivos Android e iOS, com uma solução única, abrangente e fácil de usar, em qualquer lugar, a qualquer hora.

Visite-nos no Google Play™ para experimentar todos os recursos de proteção proativos e avançados de uma assinatura do Norton Mobile Security Premium gratuita por 30 dias. Será necessário criar uma conta do Norton, sem precisar fornecer detalhes de cartão de crédito. Após o período de teste, faça o upgrade para o Premium ou continue usando os recursos gratuitos.