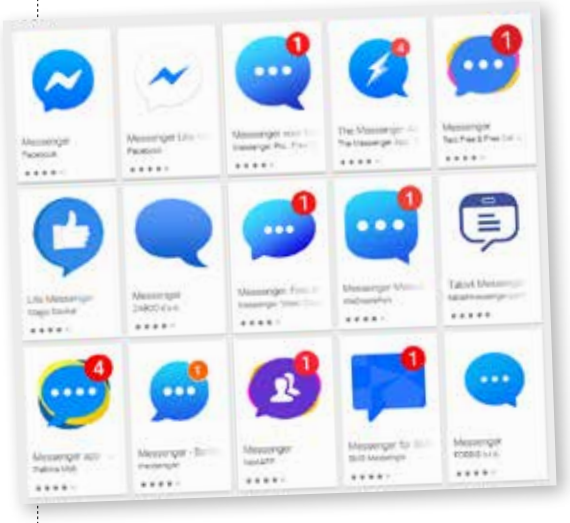
Denk je een leuke Android-app te hebben geïnstalleerd, verschijnen er vanaf dat moment schermvullende advertenties. Het is al jaren niet meer pluis in de Google Play Store. Lees over de trucs en leer veilig apps downloaden.

Tekst **Rob Schleiffert**



APP DOWNLOADEN?

PAS OP VOOR DE COPYCATS

'Nep-WhatsApp gedownload door meer dan 1 miljoen gebruikers', luidde een nieuwsbericht uit november 2017. Zocht je in die tijd in de Play Store van Google naar de populaire app WhatsApp Messenger, dan kwam je voor een lastige keus te staan. Er waren zeker vijf apps met de naam WhatsApp en met hetzelfde icoon. Er was er maar één de echte, de andere waren 'copycats'.

De app Update WhatsApp Messenger heette dankzij het woord Update net anders, maar het groene icoon was hetzelfde en de naam van de ontwikkelaar leek identiek: WhatsApp Inc. Leek, want achter Inc. stond nog een onzichtbare spatie. De filters van Google trapten erin, net als ruim een miljoen Android-gebruikers. Zij werden bedolven onder de advertenties en hun smartphone werd kwetsbaar voor nieuwe malware. Gelukkig waren er experts van buiten Google die de app ontmaskerden.

50.000 Copycats

Elke dag keurt Google duizenden malafide apps af om te voorkomen dat ze in de Play Store komen. Er glippen er ook veel tussendoor. Meestal zijn het simpele spelletjes en apps gericht op kinderen.

De na-apers vormen een groot probleem, bewees de universiteit van Sydney. Die deed twee jaar lang onderzoek door bijna 50.000 Android-apps te analyseren die erg leken op andere, populaire apps. De resultaten kwamen medio vorig jaar. Van de onderzochte copycats bleken er ruim 2000 malware te bevatten. Nog eens ruim 1500 vroegen om minstens vijf onnodige (gevaarlijke) machtigingen. En 1400 apps deelden gegevens van gebruikers met opvallend veel advertentiebedrijven.

Op welke manieren willen de makers van al die nep-apps geld verdienen? Als je de meldingen van de afgelopen jaren doorneemt, kom je tot het volgende lijstje:

1. Schermvullende advertenties tonen, soms iedere 15 minuten.
2. Klikfraude plegen: de app klikt zelf ongemerkt op advertenties en daar verdienen de appmakers aan.
3. 'Gevaarlijke' permissies vragen om zo persoonsinformatie te verzamelen, bijvoorbeeld toegang tot al je contacten. Die informatie wordt doorverkocht.
4. Ongemerkt sms-abonnementen afsluiten om de gebruiker op kosten te jagen.
5. Na een gratis testperiode de gebruiker opzadelen met een peperduur abonnement.
6. De rekenkracht van de telefoon misbruiken om bitcoins te maken.
7. De app downloadt nog meer malware, buiten Googles controle om.
8. Inlog- of betaalgegevens ontfutselen. ➜

VEILIG ANDROID-APPS DOWNLOADEN

1 Installeer alleen apps uit de **Google Play Store,** de officiële appstore van Google, of de officiële appwinkels van de telefoonfabrikanten, zoals de Galaxy Store (Samsung) en AppGallery (Huawei). Android is standaard beveiligd tegen het installeren uit andere bronnen.

2 Zijn er meerdere apps met (vrijwel) **dezelfde naam en (bijna) identiek logo**? Pas dan extra goed op.

3 Kijk **hoe vaak de app al is gedownload** en bedenk dat honderdduizend downloads nog geen zekerheid geeft. Populaire apps zijn tientallen miljoenen keren gedownload, WhatsApp zelfs al meer dan een miljard keer.

4 Check altijd de **gebruikersreviews** en let dan vooral op de negatieve recensies én hoe vaak die een duimpje hebben gekregen van andere gebruikers. Juichend positieve recensies kunnen nep zijn. Geen of heel weinig reviews? Niet installeren.

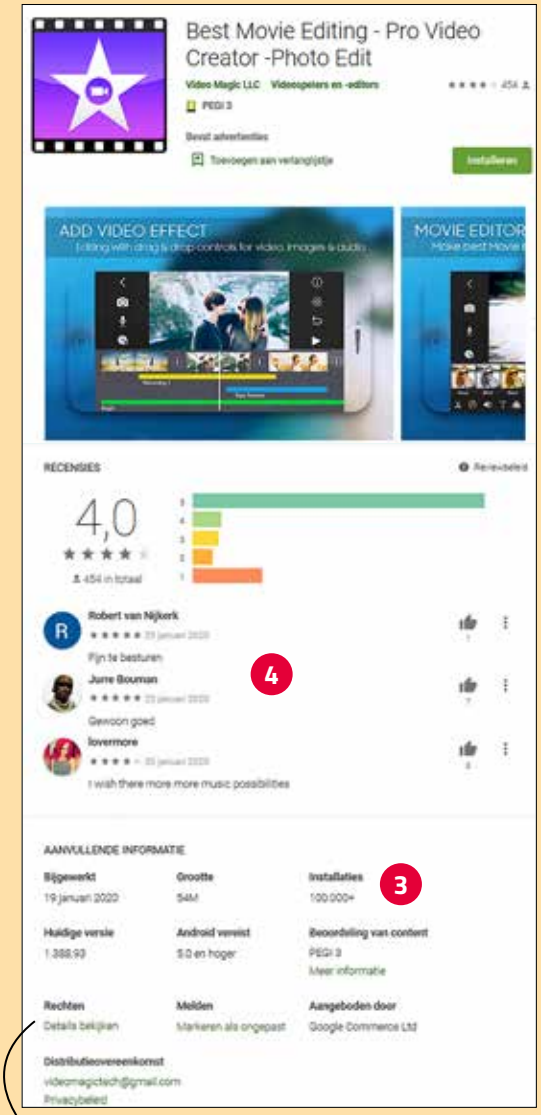
5 Controleer al in de appstore, dus vóór de installatie van een app of er **geen onnodige app-permissies** worden gevraagd. Klik op **Details bekijken** onder 'Rechten'. Het is verdacht als een foto-app sms'jes wil kunnen versturen, toegang wil tot je microfoon of altijd automatisch met de telefoon wil opstarten.

6 Kijk **wie de maker is** en in welk land die is gevestigd. Staat er geen (web)adres bij? Dat is verdacht.

7 Installeer voor extra bescherming een losse **antivirusapp**. Die van Sophos was de beste gratis app in onze test van januari 2019. Deze hield duidelijk meer tegen dan Googles Play Protect.

8 Houd je besturingssysteem (Google Android of Apple iOS) **bijgewerkt**, net als al je apps.

9 Controleer af en toe de lijst met geïnstalleerde apps en **verwijder de apps** die je niet gebruikt.



In december 2019 bevatte de Google Play Store zo'n 2,9 miljoen apps. De App Store van Apple bevatte er eind 2019 ruim 1,8 miljoen (bron: statista.com)

Vindingrijk

De vindingrijkheid van malwaremakers kent geen grenzen, blijkt uit de volgende voorbeelden. Enkele jaren geleden doken simpele apps op als zaklampen en kaartspelletjes waarmee criminelen je bankrekening konden plunderen. Na het installeren koppelde de malware in de apps zich aan de al geïnstalleerde bankapp. Wanneer de gebruiker zijn bankapp gebruikte voor een betaling, legde het virus een scherm over de app heen en kon zo de inloggegevens onderscheppen. Onder de slachtoffers waren klanten van de ING.

Vorig jaar werden ruim 200 spelletjes (meestal simulatie-apps) uit de Play Store verwijderd omdat ze stiekem malware installeerden. Na installatie vroeg zo'n app toestemming om een uitbreiding te mogen downloaden. Nadat je daarmee akkoord was gegaan, crashte de app, maar bleef de malware actief. Die kon via je browser phishingsites openen en andere apps installeren. De apps waren toen dan al zo'n 150 miljoen keer gedownload.

Apple is strenger

Apple controleert veel strenger dan Google. Iedere nieuwe app wordt handmatig door een medewerker beoordeeld. Volgens Apple wordt 40% van de apps en app-updates geweigerd, meestal omdat ze frauduleus zijn, fouten bevatten of de privacy schenden. Toch worden ook in de App Store soms foute apps ontdekt. In oktober 2019 verwijderde Apple 17 apps wegens klikfraude. Eind 2018 gooide Apple twee fitness-apps uit de App Store omdat die geld konden stelen via de creditcard van de gebruiker.

Google voert al jaren een kat-en-muis-spel met de makers van malware met de naam Bread, ook wel bekend als Joker.

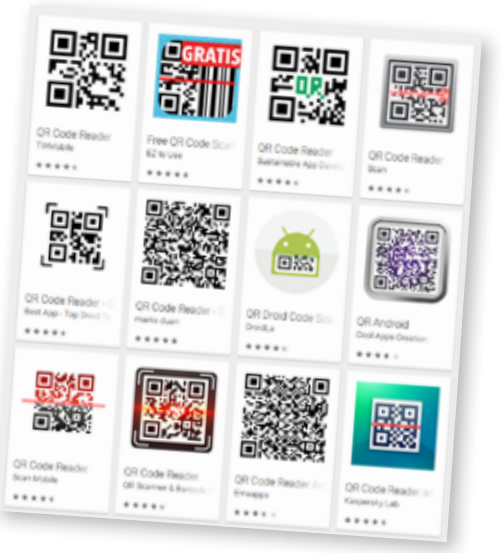
Steeds als Google besmette apps uit de appwinkel heeft geweerd (ruim 1700 keer in 3 jaar), proberen de malwaremakers het op een andere manier. Helaas lukt het af en toe om apps door de controle te krijgen. Bread zadelde de slachtoffers aanvankelijk op met dure sms-abonnementen, maar nu Google dat moeilijker heeft gemaakt, bezoekt de malware stiekem webpagina's waarvoor moet worden betaald.

Extra risico

Googles controle is nog altijd veel beter dan helemaal geen controle. Toen in de zomer van 2018 het populaire spel Fortnite verscheen, kwam het niet in de Play Store. De makers kozen ervoor om het via een eigen server aan te bieden. Je moest soms de beveiliging in Android uitschakelen om de app buiten de Play Store om te kunnen installeren. Criminelen doken er bovenop en gingen nepversies aanbieden. De gebruikers die hun beveiliging na dit avontuur niet hebben hersteld, lopen nog steeds extra risico.

Een app die alleen maar reclame toont, gooi je toch direct weg? Was het maar zo simpel. Er zijn talloze voorbeelden van apps die zich na installatie onzichtbaar maken. Hij verdwijnt uit de lijst met apps, maar blijft op de achtergrond actief om bijvoorbeeld advertentie te tonen of op sites te klikken.

Soms is niet duidelijk welke app voor problemen zorgt, omdat de malafide app pas na enkele dagen zijn ware aard laat zien. Of pas na een update. En weet je welke app je moet verwijderen, dan is die onvindbaar. Het icoon van de nep-app is dan veranderd in het icoon van bijvoorbeeld de Google Play Store.



Google doet z'n best

Met zoveel frauduleuze apps zou je haast denken dat Google alle apps ongecontroleerd doorlaat. Dat is niet zo. Volgens cijfers van Google zelf werden in 2017 meer dan 700.000 apps geweigerd of verwijderd. Meer dan een kwart miljoen daarvan waren copycats. Andere apps werden geweigerd vanwege hun aanstootgevende inhoud (zoals extreem geweld, haat en porno) of omdat ze schadelijk waren (sms-fraude, virussen of phishing). In 2018 werden zelfs nog 55% meer apps afgewezen en 66% meer apps uit de Play Store verwijderd.

Hoe werkt die controle? Volgens Google werd tot voor kort van iedere aangeboden app eerst een geautomatiseerde risicoanalyse gemaakt. Alleen twijfelgevallen werden bekeken door een medewerker. Afgelopen zomer kondigde Google aan strenger te gaan controleren. Daarvoor ging het bedrijf een samenwerkingsverband (de App Defense Alliance) aan met de internetsecuritybedrijven ESET, Lookout en Zimperium. Door de scansystemen van de vier partners te combineren, hoopt Google nu wél alle malafide apps onschadelijk te kunnen maken voordat ze in de Play Store komen.

Ondertussen verbetert Google continu het Android-besturingssysteem. Niet alle trucjes van malafide appmakers werken meer, zoals een onzichtbare laag over een andere app tonen. Helaas worden, net als bij bijna elke andere software, voortdurend nieuwe kwetsbaarheden ontdekt. ←

Consumenten bond

Digitaal bijblijven?

In de Digitaalgids vind je elke 2 maanden alles over digitale trends en online dreigingen. Probeer nu met korting.

Bekijk de aanbieding