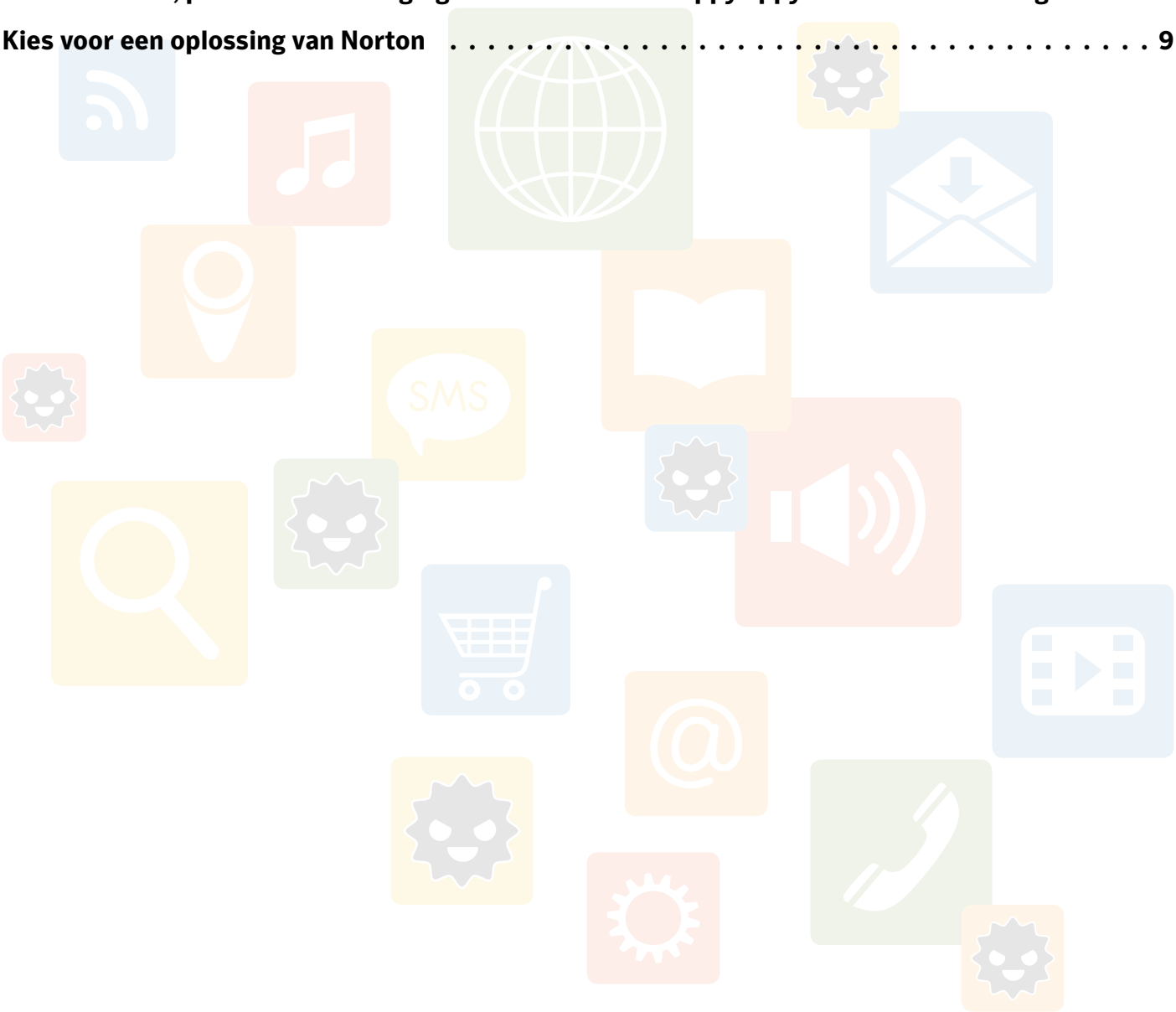
Norton by Symantec

GOED, SLECHT EN STIEKEM: WEET JIJ WAT JOUW APPS ALLEMAAL DOEN?

Apps zijn leuk, handig en gratis, maar ze kunnen je ook opzadelen met verborgen kosten en slecht gedrag. Stop met anticiperen op eventuele risico's en begin met een nieuwe, proactieve benadering van de beveiliging van je mobiele apparaten.

You Tube

Inhoud



Mobiele apparaten vind je tegenwoordig overal. Wereldwijdzijn bijna 1,8 miljard mensen, of wel een kwart van de wereldbevolking, in het bezit van een smartphone.[1] Omdat het gebruik van mobiele apparaten groeit, groeit ook het gebruik van apps.

Smartphonegebruikers over de hele wereld besteden tegenwoordig 86% van hun tijd aan het gebruik van apps en maar 14 procent aan het gebruik van het internet.[2] Wereldwijd gezien is het gemiddeld aantal geïnstalleerde apps 26 per telefoon en binnen de top 10 landen zijn het er meer dan 35.[3]

Apps geven je de vrijheid hetzelfde te doen op je mobiele apparaat als op je pc - en op nieuwe en verschillende manieren, omdat we richting het Internet of Things gaan. Zo kun je tegenwoordig al apps gebruiken om de temperatuur in je woonkamer te regelen, de lichten aan te doen voordat je thuiskomt en je huis te beveiligen tegen inbrekers.

Apps maken het mogelijk. Als je telefoon de auto is, zijn apps het stuur, het gaspedaal en de richtingaanwijzer. Ze zijn ook de sleutel waarmee je de deur opendoet naar alle informatie op je mobiele telefoon en alle informatie die je eventueel in de cloud hebt opgeslagen.

Cybercriminelen is dit niet ontgaan. Jouw persoonlijke informatie is geld waard, en hackers maken in toenemende mate gebruik van beproefde en bewezen tactieken (zoals niet-bestaande apps en ransomware) om mobiele apparaten aan te vallen. En zij zijn niet de enigen. App-ontwikkelaars die geld ruiken, zitten ook achter jouw persoonlijke gegevens aan. Hun doelstellingen zijn niet per se illegaal. Ze kunnen gewoon proberen om doelgerichte advertenties aan je informatiebalk toe te voegen. Maar hun methoden kunnen wel risico's met zich meebrengen.

Het feit dat er zo veel partijen zijn die geïnteresseerd zijn in jouw privé-informatie, maakt het des te belangrijker dat je weet wat jouw apps precies doen en dat je stappen zet die je mobiele apparaten veilig houden.

Tegenwoordig is het simpelweg lokaliseren en blokkeren van een kwijtgeraakte of gestolen telefoon niet meer voldoende. Natuurlijk bieden deze reactieve beschermende maatregelen wel belangrijke garanties. Maar de nieuwe eis is proactieve beveiliging. Dat betekent dat je niet alleen moet beveiligen tegen apps die rechtstreeks schade toe brengen door geld en persoonlijke gegevens van je stelen, maar ook een beveiliging moet hebben die je in staat stelt gefundeerde beslissingen te nemen over het potentiële risico van de apps die je downloadt en of een gratis app zijn uiteindelijke kosten waard is.

Beveiliging van mobiele telefoons vraagt nu om een preventieve benadering, zodat je met een gerust hart kunt deblokkeren en genieten van alle voordelen van onze app-gerichte wereld.

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

Weet jij wat jouw apps allemaal doen? Norton weet het wel

De meeste consumenten zijn geneigd de apps voor hun mobiele telefoon met dezelfde naïviteit te bekijken als waarmee ze 10 tot 15 jaar geleden hun desktopapplicatiesoftware bekeken. Ze installeren apps op hun telefoon en denken er niet of nauwelijks over na welke risico's dat met zich mee kan brengen. En ze installeren er een heleboel meer omdat ze met een simpele klik gedownload kunnen worden.

Apps (met name gratis apps) zijn er erg goed in je te vertellen welke voordelen ze hebben, maar ze vertellen je niet wat hun werkelijke kosten zijn. Die kosten kunnen ontstaan in de vorm van verborgen bedreigingen of andere potentiële risico's. Apple's sandboxing van hun iOS-besturingssysteem in combinatie met de sterke controle op wat er in de iTunes app store binnenkomt, maakt het moeilijk om schadelijke apps te detecteren. Maar het open karakter van het Android-besturingssysteem kan veel gemakkelijker worden gemanipuleerd om bedreigingen en potentiële risico's te veroorzaken.

The Symantec Internet Security Threat Report heeft vastgesteld dat mobiele malware in 2013 bijna uitsluitend is ontwikkeld voor de Android OS, met 32% van die apps die persoonlijke informatie van de gebruiker stelen.[4]

Daarbij mislukken bij meer dan 75% van alle mobiele apps basisbeveiligingstesten, omdat ze divers risicovol of schadelijk gedrag vertonen.[5]

En Symantec registreerde 69% stijging van gevallen van mobiele malware tussen 2012 en 2013.[6]

[4] 2014 Symantec Internet Security Threat Report: www.symantec.com/security_response/publications/threatreport.jsp
[5] Gartner: www.gartner.com/newsroom/id/2846017
[6] Norton Mobile Insight/Symantec Threat and Response monitoring and analysis data as of December 2014

Slechte apps zijn ook echt slecht

Het is eenvoudig vast te stellen waarom mobiele apps zo aantrekkelijk zijn voor hackers. Het aantal gebruikers groeit snel en de hoeveelheid informatie die beschikbaar komt zodra een schadelijke app is geïnstalleerd is enorm. En zoals altijd worden hackers steeds beter. Ze leren en delen informatie, en hun aanvallen worden steeds intelligenter. Cybercriminelen brengen hun betrouwbare computertactieken (zoals phishing, fake software en ransomware) over op mobiele telefoons.

In één van de vervalste app-oplichtingen, boden phishers een valse app aan die beweerde gratis belminuten te leveren. Het aanbod was alleen geldig als een gebruiker zijn of haar inloggegevens invoerde en het aanbod naar 10 vrienden doorstuurde. Het lukte de oplichters om het aantal slachtoffers exponentieel te vergroten. Hun inloggegevens werden gestolen en andere persoonlijke gegevens werden buitgemaakt.

Een andere valse app maakte een exacte kopie van de Mizrahi Bank, een van de grootste banken in Israël. Hackers uploaden deze naar de Google Play store waar hij vervolgens door nietsvermoedende klanten van de bank werd gedownload. Bij het openen van de app en het invullen van de inloggegevens werden hun gebruikers-ID's ingenomen. Vervolgens stuurde de app op slinkse wijze een foutmelding en gaf de klanten instructies om de echte app van de bank opnieuw te installeren met de belofte dat deze daarna prima zou werken. De meeste klanten hadden er helemaal geen weet van dat hun gebruikers-ID ooit was gestolen.

Een andere recente bedreiging is Android. Simplocker, een Trojaans paard dat binnenkomt via een valse app. Zodra deze eenmaal is geïnstalleerd op je apparaat, codeert (of blokkeert) hij bestanden, toont vervolgens een valse waarschuwing van justitie waarin staat dat er illegaal pornografisch materiaal op je apparaat is gevonden. Maar als je een "boete" van 300 US dollar betaalt via de betalingsservice MoneyPak zullen je bestanden worden gedeblokkeerd.

Beknopte handleiding schadelijke apps

Meer dan 20% van de 15 miljoen apps die zijn geanalyseerd door Norton zijn schadelijke apps.[7] Ze duiken op in heel veel verschillende vormen:

Tracking-apps verzamelen tekstberichten en gespreksverslagen, volgen GPS-coördinaten en halen foto's en filmpjes van apparaten. Het rapport van Norton van 2014 liet zien dat het aantal bedreigingen als gevolg van het volgen van gebruikers in 2013 is gestegen van 15 naar 30%.

Stealing-apps Stealing-apps verzamelen apparaat- en gebruikersspecifieke data zoals configuratiedata en persoonlijke informatie.

Infectie-apps maken gebruik van traditionele malwarefuncties zoals het installeren van backdoors en downloaders waardoor hackers toegang tot je telefoon krijgen.

Reconfiguratie-apps vergroten de privileges of bewerken instellingen in het besturingssysteem die de weg vrij kunnen maken voor aanvallers.

Money-theft-apps gebruiken nummers van tekstberichten met een verkorte code of premium-rate. Vervolgens maken hackers malware die tekstberichten naar die nummers sturen vanaf geïnfecteerde apparaten. De gebruiker betaalt de factuur en de hacker krijgt het geld.

Two-factor theft apps kunnen een tekstbericht van jouw bank onderscheppen met daarin een eenmalige authentificatiecode waarmee hackers toegang tot jouw bankrekening kunnen krijgen.

[7] Norton Mobile Insight/Symantec Threat and Response monitoring and analysis data as of December 2014

Grayware kan ook gevaarlijk zijn

De scheidslijn tussen legitieme software en malware is niet heel duidelijk. Er bestaat een groep apps die bekend staan als *grayware* en deze nemen een grijs gebied in beslag. In dit grijze gebied werken een heleboel ongevaarlijke ontwikkelaars die het gemakkelijk vinden om gebruikers over te halen potentieel gevaarlijke apps te downloaden die informatie en content openbaar maken vaak door gebruik te maken van een “gratis” app.

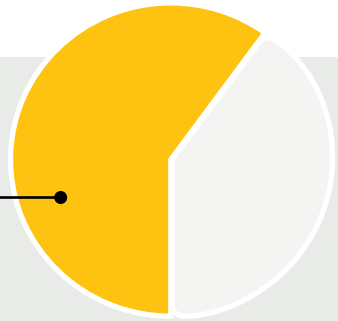
Hoewel grayware-apps geen schadelijke code bevatten, kunnen ze nog steeds inbreuk doen op je privacy en je telefoon besmetten met advertenties en allerlei ander vervelend gedrag. Een veel voorkomende type *grayware* genaamd *mobile adware*, of *madware*, omvat apps die advertenties weergeven in de meldingsbalk, de ringtone vervangen door gesproken advertenties of, nog erger, privégegevens zoals telefoonnummers of gebruikersaccountinformatie openbaar maken.

Je zou een heleboel van deze risico’s kunnen zien als je behoorlijk wat technische kennis hebt en je de lange lijst van app-bevoegdheden waarmee je akkoord gaat grondig doorleest voordat je een app download van de Google Play store.

Onderzoek van Norton laat zien dat meer dan

60%

van Android-apps adware of andere grayware bevat.[8]



Maar dat gebeurt niet altijd. Zelfs als je de voorwaarden doorleest, weet je nog steeds niet al het actuele gedrag van de app.

Als grayware eenmaal is geïnstalleerd, kan het je locatie volgen of je internetgedrag controleren en deze informatie aan marketeers verkopen. In veel gevallen heeft een app een redelijk excuus voor het verzamelen van sommige gevoelige informatie, maar normaal gesproken ben je je niet bewust van dat gedrag en vind je het misschien niet prettig dat bepaalde persoonlijke informatie gedeeld wordt met die speciale app. Neem bijvoorbeeld een app die jouw telefoonnummer als een unieke ID van je telefoon haalt en het via het netwerk verspreidt zonder codering. Dan is je telefoonnummer plotseling overal virtueel beschikbaar voor marketeers en oplichters.

Of een app kan een potentieel privacyrisico vormen door informatie te verzamelen die niet relevant lijkt gezien het doel van de app. Waarom zou een weerapp bijvoorbeeld toegang moeten hebben tot jouw contacten of agenda?

Even gebruikelijk zijn apps die veel stroom gebruiken, de prestaties van het apparaat verminderen, of gegevens van het netwerk downloaden waardoor je rekening flink oploopt. Deze apps zijn weliswaar technisch gezien geen grayware, maar wel heel vervelend. Veel van deze apps werken heimelijk op de achtergrond. Valt het je op dat je batterij eerder leeg is naarmate je je telefoon langer hebt? Dat kan het gevolg zijn van apps. Zijn je rekeningen ineens onverwacht hoog? Ook hier geldt: apps. Veel van hen zijn constant aan het downloaden, zelfs als je ze niet hebt geopend.

[8] Norton Mobile Insight/Symantec Threat and Response monitoring and analysis data as of December 2014

Norton biedt vooraanstaande beveiliging voor je mobiele telefoon

Je vertrouwt Norton op je computer. We passen dezelfde grensverleggende technologie, diepgaand onderzoek en wereldwijde intelligentiebronnen toe om je mobiele apparaat te beveiligen.

De meeste beveiligingsprogramma's van tegenwoordig bieden basisbebeveiliging.

Wij gaan op mobiel terrein een stapje verder om technologie te kunnen leveren die jou voorziet van volledige bescherming tegen schadelijke en vervelende apps. Wij gebruiken onze 30 jaar ervaring op het gebied van beveiliging plus de grootste bedreigingendatabase ter wereld om jou te helpen je te beschermen tegen bedreigingen van Android-apps.

Norton Mobile Insight werkt dag en nacht

Alle gegevens over Android-apps die wij verzamelen via Norton Mobile Insight – door regelmatig meer dan 200 app stores te onderzoeken en app-informatie te halen van het Norton Community Watch netwerk – worden in ons systeem ingevoerd en gaan door een grote hoeveelheid programma's om die apps te identificeren die problemen veroorzaken.

We beginnen met een statische analyse die inhoudt dat we basisgegevens verzamelen zoals de naam van de app, de handtekening van de ontwikkelaar en de lijst met bevoegdheden, die meestal wordt getoond op het moment dat een app gedownload wordt en die uitzonderlijk lang kan zijn.

Daarna graven we wat verder naar de code van de app om te zien welke gevoelige applicatie programma interfaces (API's) zullen worden opgeroepen. Bijvoorbeeld of de app API's oproept om jouw telefoonnummer en andere privé-informatie te kunnen lezen en vervolgens toegang tot het internet heeft. En we gaan nog verder. We zoeken uit of de app gelokaliseerd is. Wordt hij geïnstalleerd zonder dat er een pictogram op de startbalk wordt gezet? Deze informatie levert belangrijke gegevens over de veiligheid van de app.

Vervolgens voeren we een belangrijke dynamische analyse uit die ons een buitengewoon zicht geeft op de privacy en het lekken van informatie door de app. We halen elke app door een instrumentele Android-emulator waardoor de app denkt dat hij in de echte wereld actief is. Als een app bijvoorbeeld informatie over het apparaat of persoonlijke informatie op de achtergrond verzamelt en verzendt, zou deze naar een ongewenste derde kunnen gaan.

Wij voeren deze analyse uit op een intelligente, geautomatiseerde manier door werkelijke gebruiksstromen en -functies te testen. Veel van onze concurrenten herleiden simpelweg het gedrag van apps en rapporteren risico's op basis van app-bevoegdheden zonder daadwerkelijk te testen, wat kan leiden tot onnauwkeurige informatie of valse alarmmeldingen naar de gebruiker.

Onze exclusieve mobile intelligence-technologieën en bronnen omvatten het volgende:

Norton™ Mobile Insight is een dynamisch systeem dat constant nieuwe of bijgewerkte Android-apps download en analyseert van meer dan 200 app stores, inclusief Google Play, om unieke, constante app-intelligence te kunnen genereren. Wij analyseren elke dag meer dan 30.000 nieuwe apps en hebben tot nu toe meer dan 15 miljoen apps geanalyseerd.

Norton Community Watch is een levendig netwerk, bestaande uit miljoenen gebruikers die ons toestaan anonieme meta- en prestatiegegevens te verzamelen van de apps op hun Android-telefoons, inclusief vele eerder niet ontdekte app-bestanden Door gebruik te maken van deze communitygegevens en realtime analyses te maken, biedt Norton Mobile Insight een andere manier om het gedrag van een app te begrijpen zodra deze is geïnstalleerd, en van de risico's die je loopt door de app op je telefoon te laten staan. In feite is 25% van de bekende apps die zijn geanalyseerd door Norton Mobile Insight verzameld door Norton Community Watch, wat betekent dat we een heleboel apps analyseren en leren kennen die niet verspreid zijn via app stores.

De Symantec Security Technology and Response (STAR)-divisie is een wereldwijde groep van beveiligingstechnici, virusjagers, bedreigingsanalisten en onderzoekers die de onderliggende beveiligingstechnologie, content en ondersteuning leveren voor alle Symantec beveiligingsproducten, inclusief die voor mobiele telefoons. Deze experts zijn onze ogen en oren, die de wereld van de bedreigingen dag en nacht in de gaten houden om jou te beschermen.

Data: hoe meer je hebt, hoe meer je weet

Uiteindelijk levert de Norton-oplossing een duidelijk voordeel van de Symantec Data Analytics Platform (SDAP) op één van de zeldzame systemen dat krachtig en flexibel genoeg is om die enorme groei van cyberbedreigingen, mobiele en andere bedreigingen voor te blijven.

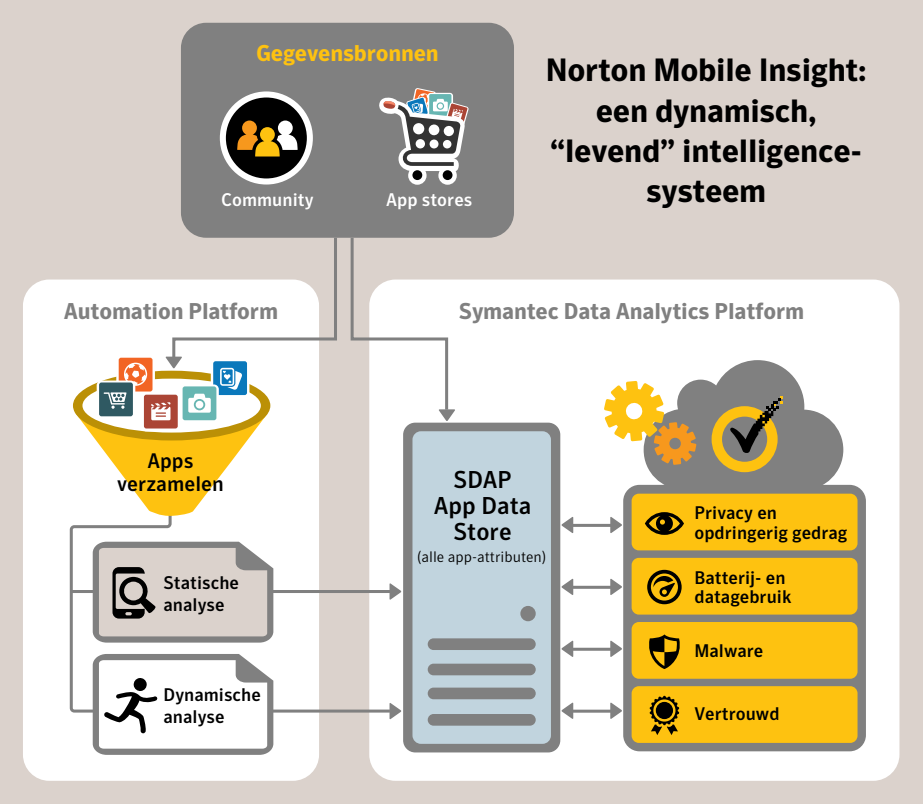
Het SDAP-platform is een enorme, steeds groeiende database met al onze beveiligingsgegevens. Onze mobiele gegevens omvatten rond de 1,6 miljard individuele stukjes van gegevens. Dat is erg veel. Maar dat is nodig om jouw apparaat te beveiligen tegen mogelijke bedreigingen.

Alle app-gegevens die we verzamelen, van gedrag tot stabiliteit en prestatiedetails, worden verwerkt door het SDAP-platform. Deze gegevens bevatten informatie over de prestaties van de app in de echte wereld, hoeveel mensen in Norton Community Watch deze app hebben gebruikt, in welke app stores je hem vindt en hoeveel mensen hem hebben gedownload.

Wij analyseren al die gegevens en bepalen op basis daarvan of de app schadelijk is of niet. Norton Mobile Insight heeft tot nu toe meer dan 15 miljoen apps verwerkt en verwerkt elke dag opnieuw 30.000 nieuwe apps. Het detecteert de kenmerken en patronen die duiden op malware, het controleert apps op verdachte inbreuk op de privacy en opdringerig gedrag en het test de batterij en het datagebruik.

En het wordt steeds slimmer, omdat de wereld van de bedreigingen verandert. Het leert en ontwikkelt zich op basis van de nieuwe gegevens die het verzamelt. Het weet bijvoorbeeld dat een app in malware meestal kleiner is dan in niet-schadelijke apps, omdat de meeste malwareontwikkelaars niet veel tijd besteden aan de verfijning van hun product.

Norton Mobile Insight vergelijkt al deze informatie vervolgens met honderden andere datapoints om te kijken of de app malware is en stelt een betrouwbaarheidsniveau in voor de veiligheid van de app in. Het herkent elementen die inherent zijn aan malware die een aanvaller niet eenvoudig kan wijzigen, zoals codepatronen, technieken voor het vertonen van schadelijk gedrag en de status van de reputatie van de ontwikkelaar binnen de community.



Geavanceerde, proactieve beveiliging is noodzakelijk in de happy appy-wereld van vandaag

Norton Mobile Security is een krachtige, op het internet gebaseerd productabonnement ontworpen om jou en je mobiele apparaten te beschermen. Het is mogelijk gemaakt door de geavanceerde technologie van Norton Mobile Insight zoals besproken in dit document. Norton Mobile Security is ontworpen om jou tijd te besparen en om de onzekere factor bij het identificeren van apps met alle risico's weg te nemen.

De sleutel tot Norton Mobile Security is een functie die de app scant, de App Advisor.

Mogelijk gemaakt door Norton Mobile Insight, biedt de App Advisor je proactieve beveiliging door je apps automatisch te laten scannen op Google Play VOORDAT je ze downloadt (op Android 4.0 of hoger, of Android 4.2 of hoger op Samsung-apparaten). Het vertelt je of je apps een schadelijke code bevat of dat ze privacyrisico's, opdringerig gedrag of hoog batterij- of dataverbruik met zich meebrengen. Het scant ook automatisch je eerder gedownloade Android-apps of geïnstalleerde apps van buiten een app store op dezelfde risico's en biedt je de mogelijkheid ze desgewenst te verwijderen.

Met één simpele stap kun je gemakkelijk weloverwogen kiezen voor Android-apps. Je kunt zelf beslissen of een bepaalde app het "geld" waard is.

Norton Mobile Security levert ook andere proactieve beveiligingsonderdelen voor jou en je Android-apparaten, zoals internetbeveiliging om je te beschermen tegen frauduleuze websites die zijn ontwikkeld met het doel je persoonlijke informatie en je geld te stelen. Het bevat ook recovery op afstand voor je Android-apparaat, iPhone en iPad, zodat je ze snel kunt vinden. Je kunt zelfs contactgegevens opslaan en deze weer herstellen wanneer je apparaat wordt gestolen of je het kwijtraakt. Nu is het heel eenvoudig om al je apparaten te beschermen met één enkel internetabonnement. Norton Mobile Security de krachtige potentie van mobiele vrijheid en comfort ondervinden, maar wel veilig.

Kies voor een oplossing van Norton

Mobiliteit is een integraal onderdeel van jouw drukke, online bestaan. Maar door de betrouwbaarheid van deze kleine computers, je mobiele apparaten, te vergroten is het een vereiste dat je je realiseert welke risico's je loopt en dat je stappen zet om jezelf te beschermen.

Wij bieden ook Norton Mobile-beveiligingsstechnologieën als een onderdeel van ons platform Norton Security en Norton Security with Backup-abonnementen.

Deze abonnementen leveren jou en, je gezin beveiliging op maat voor je pc's, Macs, Android- en iOs-apparaten met een gemakkelijk in het gebruik zijnde totaaloplossing, op elk moment, waar je ook bent.

Bezoek ons op Google Play™ de geavanceerde kenmerke van een Norton Mobile Security Premium-abonnement zelf gedurende 30 dagen gratis uit te proberen. Je hoeft alleen maar een Norton-account aan te maken, je creditcard is niet nodig. Na afloop van de proefperiode, kun je upgraden naar de premiumversie of de gratis functies blijven gebruiken.