Norton by Symantec

OUTIL, DANGER, OU FAUX-SEMBLANT : SAVEZ-VOUS CE QUE VOS APPLICATIONS FONT EXACTEMENT ?

Les applications gratuites sont attrayantes et efficaces, mais elles peuvent aussi engendrer des coûts cachés et se comporter de façon suspecte. Plutôt que de réagir aux risques, adoptez une nouvelle approche de la protection mobile.

You Tube

Sommaire

Les appareils mobiles intelligents sont aujourd'hui omniprésents : près de 1,8 milliard de personnes sur la planète, soit un quart de la population mondiale, possèdent un smartphone.[1] Cet essor des appareils mobiles va de pair avec une utilisation croissante des applications.

Les utilisateurs de smartphones du monde entier passent désormais 86 % de leur temps sur des applications, et à peine 14 % sur le Web.[2] On compte en moyenne 26 applications installées par smartphone à l'échelle mondiale, et plus de 35 dans les 10 pays les plus importants.[3]

Les applications sont synonymes de liberté parce qu'elles permettent de faire les mêmes choses sur un appareil mobile que sur un PC. Elles apportent même de nouvelles habitudes à mesure que l'Internet des objets se dessine. Par exemple, vous pouvez déjà utiliser des applications pour contrôler la température ambiante de votre salon, allumer les lampes avant de rentrer chez vous et protéger votre domicile contre les intrusions.

Les applications sont des instruments. Si votre téléphone était un véhicule, les applications seraient le volant, l'accélérateur et le clignotant. Elles sont également la clé qui vous donne accès aux informations stockées sur votre appareil mobile, et à toutes celles que vous placez dans le cloud.

Les cybercriminels l'ont bien compris : vos informations personnelles valent de l'argent. De plus en plus, les pirates ciblent les appareils mobiles à l'aide de techniques éprouvées (fausses applications et autre ransomware). Et ils ne sont pas les seuls. Des développeurs attirés par l'appât du gain en veulent également à vos données. S'ils ne le font pas forcément à des fins illicites – ils chercheront simplement à insérer des publicités ciblées dans votre barre de notification, par exemple – leurs méthodes présentent des risques.

Face à une telle convoitise, il devient essentiel de savoir ce que les applications que vous installez font de vos données privées et de prendre les mesures nécessaires pour sécuriser vos appareils mobiles.

En cas de perte ou de vol, on ne peut plus aujourd'hui se contenter de localiser et verrouiller l'appareil. Certes, ces mesures de protection sont des précautions importantes, mais la sécurité préventive constitue un nouvel impératif. Cette protection ne vise pas seulement à contrer les applications malveillantes qui dérobent de l'argent et des données personnelles, elle vous donne les moyens de prendre des décisions éclairées sur le danger potentiel des applications que vous téléchargez, et de déterminer si la gratuité de l'application compense le coût qu'elle pourrait avoir.

À l'heure actuelle, la protection mobile impose d'adopter une nouvelle approche pour que vous puissiez bénéficier en toute confiance des atouts de cet univers axé sur les applications.

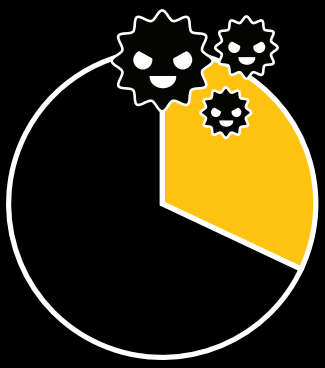
[1] eMarketer : www.emarketer.com/Article/Worldwide-Smartphone-Usage-Grow-25-2014/1010920
[2] Flurry : www.flurry.com/bid/109749/Apps-Solidify-Leadership-Six-Years-into-the-Mobile-Revolution#.VH5uBmctDIU
[3] Our Mobile Planet : www.think.withgoogle.com/mobileplanet/en/

Savez-vous ce que font vos applications exactement ? Nous le savons.

La plupart des consommateurs affichent la même naïveté vis-à-vis des applications mobiles qu'ils le faisaient voici 10 ou 15 ans avec les logiciels pour PC. Ils les installent sans guère se soucier des risques qu'ils prennent ainsi, d'autant plus que quelques clics suffisent pour effectuer un téléchargement.

Les applications, en particulier celles qui sont gratuites, savent très bien vous annoncer leurs avantages, mais elles oublient de vous indiquer le coût qu'elles représentent réellement, notamment en termes de menaces cachées et autres risques potentiels. Grâce à la stratégie d'isolement, ou sandboxing, adoptée par Apple pour protéger son système d'exploitation iOS, et les contrôles rigoureux que l'éditeur impose aux applications proposées sur l'App Store, il est peu probable de tomber sur une application malveillante. Mais le système d'exploitation Android, ouvert par nature, peut être plus facilement manipulé dans le but de propager des menaces et des risques potentiels.

Dans son rapport sur la sécurité Internet, Symantec a montré qu'en 2013 les applications mobiles malveillantes ont été presque exclusivement développées pour l'OS Android, et 32 % de ces applications visaient à dérober les informations personnelles de l'utilisateur.[4]



En outre, plus de 75 % de toutes les applications mobiles échouaient aux tests de sécurité élémentaires parce qu'elles présentaient divers comportements malveillants ou à risque.[5]

Symantec a également enregistré une hausse de 69 % du nombre de programmes mobiles malveillants entre 2012 et 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] Données d'analyse et de surveillance de Norton Mobile Insight/Symantec Threat and Response au mois de décembre 2014

Une application dangereuse n'a pas d'autre finalité

On comprend facilement pourquoi les applications mobiles présentent un tel intérêt pour les pirates. Le nombre d'utilisateurs grimpe en flèche et la quantité d'informations accessibles, une fois l'application installée, est considérable. Et les pirates sont de plus en plus efficaces, c'est en quelque sorte leur mission. Ils se familiarisent avec les techniques et échangent leurs connaissances, si bien que leurs attaques sont de plus en plus sophistiquées. Les cybercriminels adaptent les tactiques mises au point pour les PC (tels le phishing, les faux logiciels et les ransomware) pour les téléphones mobiles.

Dans une fausse application, des phisheurs promettaient des minutes de communication mobile gratuites. Pour profiter de l'offre, l'utilisateur devait saisir ses identifiants de connexion et transmettre l'offre à 10 amis. La fraude avait pour but d'accroître de façon exponentielle le nombre de victimes, dérobant leurs identifiants de connexion et récoltant du même coup d'autres données personnelles.

Dans un autre cas, une fausse application imitait avec exactitude l'application de l'établissement bancaire Mizrahi Bank, l'un des plus importants d'Israël. Les pirates ayant placé l'application sur la plate-forme d'achat Google Play, les clients de la banque la téléchargeaient sans se douter de rien. Lorsqu'ils ouvraient l'application et saisissaient leurs identifiants, l'application subtilisait ces informations. Elle envoyait alors un message d'erreur intimant aux clients de réinstaller l'application authentique, qui fonctionnait alors très bien. La plupart des clients ne se doutaient pas un instant du vol dont ils venaient d'être victimes.

Plus récemment, une autre menace a touché le système Android : le cheval de Troie Simplocker, qui se propage par le biais d'une fausse application. Une fois installé sur l'appareil, il chiffre (ou verrouille) les fichiers, puis affiche une prétendue alerte du FBI signalant la détection de contenus pornographiques illicites sur l'appareil. Pour déverrouiller ses fichiers, l'utilisateur est incité à s'acquitter d'une amende de 300 dollars via un système de paiement appelé MoneyPak.

Guide pratique des applications malveillantes

Plus de 20 % des 15 millions d'applications analysées à ce jour par Norton sont malveillantes.[7] Elles servent différents objectifs

Suivi – ces applications collectent les SMS et les journaux d'appel, pistent les coordonnées GPS, enregistrent les appels et subtilisent les photos et vidéos stockées sur l'appareil. Le rapport Norton 2014 a établi que le volume de ces menaces est passé de 15 à 30 % en 2013.
Le rapport Norton 2014 a établi que le volume de ces menaces est passé de 15 à 30 % en 2013.

Vol de données – ces applications collectent des données propres à l'appareil et à l'utilisateur : informations sur l'appareil, données de configuration et contenus personnels.

Infection – ces applications jouent le rôle classique des programmes malveillants : installation de portes dérobées et de téléchargeurs qui permettent aux pirates d'accéder à votre appareil.

Reconfiguration – ces applications relèvent les niveaux de privilège ou modifient le paramétrage du système d'exploitation qui devient alors accessible aux auteurs d'attaques.

Vol d'argent – ces applications utilisent des numéros courts pour l'envoi de SMS à un tarif élevé. Les pirates créent ensuite un programme malveillant qui envoie des messages à ces numéros à partir d'appareils infectés. Les utilisateurs reçoivent la facture de l'opérateur, tandis que les pirates profitent des fonds ainsi récoltés.

Vol par authentification bifactorielle – ces applications peuvent intercepter un SMS de votre banque comportant un code d'authentification à usage unique, grâce auquel les pirates peuvent accéder à votre compte bancaire.

[7] Données d'analyse et de surveillance de Norton Mobile Insight/Symantec Threat and Response au mois de décembre 2014

Le grayware, autre source de risque

La différence entre logiciels légitimes et programmes malveillants n'est pas clairement définie. Entre les deux, une catégorie d'applications, communément appelée *grayware*, forme une zone trouble occupée par de nombreux développeurs malveillants pour qui il est facile de convaincre les mobinautes de télécharger des applications susceptibles de mettre en danger leurs informations et leurs contenus, bien souvent en les appâtant avec une application « gratuite ».

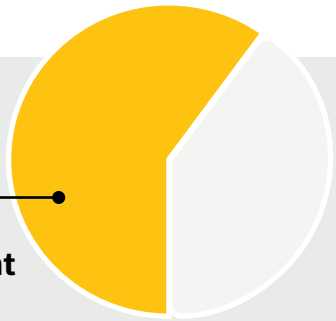
Le grayware ne contient pas de code malveillant, mais il peut quand même porter atteinte à votre vie privée, vous imposer l'affichage de publicités et modifier le fonctionnement de votre appareil de façon gênante. Un type courant de *grayware*, appelé *mobile adware* ou *madware*, compte des applications qui affichent des publicités dans la barre de notification du téléphone, remplacent la tonalité par des annonces vocales ou, pire, divulguent des données privées comme le numéro de téléphone ou les informations relatives au compte de l'utilisateur.

Avec quelques connaissances techniques et en lisant attentivement la longue liste des autorisations que vous accordez aux applications au moment du téléchargement de l'application sur Google Play, vous devriez parvenir à détecter une bonne partie de ces risques.

Les études menées par Norton montrent que

60 %

des applications Android contiennent un adware ou autre grayware.[8]



Mais ce n'est pas toujours le cas. Même si vous vérifiez les autorisations, vous ne connaissez pas tous les aspects du comportement réel de l'application.

Une fois installé, le grayware peut suivre votre position géographique ou surveiller les pages Web que vous consultez et vendre ces informations à des professionnels du marketing. Dans bien des cas, l'application offre un prétexte raisonnable pour recueillir certaines informations sensibles, mais en général vous n'avez pas connaissance de son comportement. Et si vous l'étiez, vous ne seriez probablement pas prêt à communiquer certaines informations personnelles à l'application. Prenons par exemple une application qui collecte votre numéro de téléphone pour identifier votre appareil et envoie cette information sur le réseau sans la chiffrer. Votre numéro se retrouve soudain à la portée des professionnels du marketing et des fraudeurs.

Une application peut également présenter un risque de confidentialité si elle collecte des informations qui semblent sans rapport avec son utilité. Par exemple, pourquoi une application météo aurait-elle besoin d'accéder à vos contacts et à votre agenda ?

D'autres applications tout aussi courantes vident la batterie, pèsent sur les performances de l'appareil ou téléchargent à outrance et font exploser votre facture. Techniquement, ces applications ne tombent pas dans la catégorie du grayware, mais leur comportement est assurément gênant. Nombre d'entre elles fonctionnent en arrière-plan, à la dérobée. Avez-vous remarqué que l'autonomie de votre batterie se réduisait comme peau de chagrin au fil du temps ? Cela vient peut-être des applications. Vos frais de connexion aux données sont plus élevés que prévu ? Là encore, les applications y sont sans doute pour quelque chose. Dans bien des cas, elles effectuent des téléchargements même quand elles sont fermées.

[8] Données d'analyse et de surveillance de Norton Mobile Insight/Symantec Threat and Response au mois de décembre 2014

Norton adapte la protection de pointe au mobile

Vous faites confiance à Norton pour protéger votre PC. Sachez que nous mobilisons les mêmes technologies de pointe, structures de recherche et sources d'information mondiales pour sécuriser votre appareil mobile.

Aujourd'hui, la plupart des produits de sécurité mobile sur le marché proposent une protection de base.

Nous allons plus loin en vous offrant une protection complète contre les applications mobiles malveillantes et gênantes. Nous nous appuyons sur nos 30 années d'expérience en matière de sécurité et sur la plus vaste base de données des menaces au monde pour vous mettre à l'abri des risques associés aux applications Android.

Norton Mobile Insight : une veille de tous les instants

Norton Mobile Insight nous permet de recueillir des données sur les applications Android en passant au crible plus de 200 plates-formes de téléchargement et en compilant les informations issues de la Communauté de veille Norton. Toutes ces données sont ensuite traitées par un ensemble d'outils robustes afin d'identifier les applications qui posent problème.

Nous commençons par une analyse statique, avec extraction de données élémentaires telles que l'intitulé de l'application, la signature du développeur et la liste des autorisations requises, généralement affichée lors du téléchargement de l'application et parfois excessivement longue.

S'ensuit un examen approfondi du code de l'application, pour identifier les interfaces de programmation (ou API, Application Program Interface) qu'il doit exploiter. Par exemple, l'application appellera-t-elle des API pour lire votre numéro de téléphone et autres informations privées, puis pour accéder à Internet ? Mais l'interrogatoire ne s'arrête pas là. Nous déterminons si l'application utilise la localisation et si elle s'installe sans placer d'icône dans l'exécuteur. Ces informations fournissent d'excellentes indications sur la sécurité de l'application.

Ensuite, nous procédons à une importante analyse dynamique qui offre une vision complète de la confidentialité de l'application et des fuites d'information. Nous exécutons chaque application dans un émulateur Android instrumenté pour fournir à l'application des conditions d'exploitation réelles. Par exemple, si l'application collecte et transmet en arrière-plan des informations sur l'appareil ou l'utilisateur, il est possible que ces données parviennent à des tiers indésirables.

Cette analyse suit un protocole automatisé et intelligent qui repose sur des schémas d'utilisation et des fonctions réelles. Nombre de nos concurrents se contentent de déduire le comportement des applications mobiles et de documenter les risques sur la seule base des autorisations demandées, sans véritables tests, avec le risque de transmettre des informations erronées ou de fausses alertes aux utilisateurs.

Technologies et ressources exclusives de Norton pour le mobile :

Norton™ Mobile Insight est un système dynamique qui télécharge et analyse en permanence les applications Android et leurs mises à jour sur plus de 200 plates-formes de téléchargement, dont Google Play, pour constituer en continu une source de renseignements exclusive. Nous traitons plus de 30 000 nouvelles applications par jour et avons à ce jour analysé plus de 15 millions d'applications.

La Communauté de veille Norton est un réseau actif grâce auquel nous recueillons des métadonnées anonymes et des données de performance à partir des applications exécutées sur les appareils Android de plusieurs millions d'utilisateurs, et notamment sur des fichiers application passés inaperçus jusqu'ici. Fort de ces données analysées en temps réel, Norton Mobile Insight peut étudier sous un autre angle le comportement des applications après leur installation, ainsi que les risques encourus si elle demeure sur l'appareil. En fait, la Communauté de veille Norton collecte à elle seule 25 % des applications connues et analysées par Norton Mobile Insight, ce qui signifie que nous analysons et étudions de nombreuses applications non diffusées sur les plates-formes de téléchargement.

La division Symantec Security Technology and Response (STAR) est une équipe mondiale d'ingénieurs en sécurité, de chasseurs de virus, d'analystes des menaces et de chercheurs qui fournissent la technologie de sécurité sous-jacente, les contenus et le support nécessaires à tous les produits de sécurité Symantec, dont la gamme mobile. Ces spécialistes sont nos yeux et nos oreilles. Jour et nuit, ils passent en revue les menaces existantes pour vous protéger.

Données : quand le volume fait la force

La solution Norton offre enfin un atout de taille : Symantec Data Analytics Platform (SDAP), l'un des rares systèmes dotés de la puissance et de l'agilité suffisantes pour faire face à la croissance phénoménale des cybermenaces, mobiles ou autres.

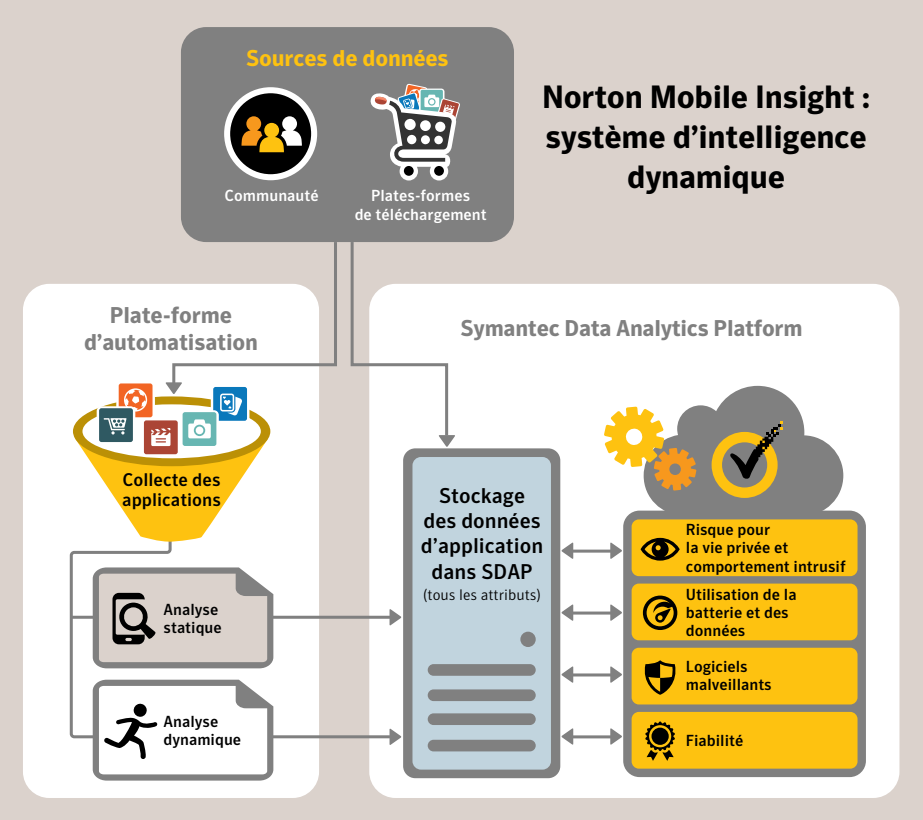
La plate-forme SDAP est une base de données immense et en constante expansion qui abrite l'ensemble de nos données relatives à la sécurité. Dans le domaine du mobile, nos disposons d'environ 1 600 milliards de données. Un volume certes colossal, mais indispensable pour protéger votre appareil contre les menaces mobiles.

SDAP traite l'intégralité des données que nous collectons sur le comportement des applications, leur stabilité et leur impact sur les performances, notamment : fonctionnement de l'application dans un environnement réel, nombre d'utilisateurs au sein de la Communauté de veille Norton, plates-formes de téléchargement qui la distribuent et nombre de personnes qui l'ont téléchargée.

Après analyse de toutes les données, nous déterminons si l'application est malveillante. Norton Mobile Insight a déjà traité plus de 15 millions d'applications et analyse 30 000 nouvelles applications chaque jour. Nous détectons les fonctions et schémas de fonctionnement caractéristiques des programmes malveillants, nous recherchons les comportements intrusifs ou portant potentiellement atteinte à la vie privée et nous examinons l'utilisation de la batterie et des données.

À mesure que le paysage des menaces évolue, le système devient plus intelligent. Il apprend et s'adapte en fonction des nouvelles données collectées. Il sait, par exemple, que les applications malveillantes sont généralement de taille plus réduite que les applications fiables, parce que dans le premier cas, les développeurs ne perdent pas de temps à affiner leurs créations.

Norton Mobile Insight recoupe ensuite toutes ces informations avec des centaines de points de données différents, puis détermine le niveau de fiabilité de la sécurité de l'application. Il reconnaît les éléments inhérents aux programmes malveillants que le développeur peut difficilement modifier (comme les séquences de code fréquentes), les techniques de déclenchement des comportements malveillants, ainsi que la réputation du développeur au sein de la communauté.



Une protection proactive avancée est indispensable dans l'univers actuel des applications

Norton Mobile Security est une puissante solution par abonnement conçue pour vous protéger et sécuriser vos appareils mobiles. Ce produit repose sur la technologie de pointe Norton Mobile Insight, présentée dans ce document. Norton Mobile Security est conçu pour vous faire gagner du temps et vous aider à identifier avec certitude les applications présentant tous les risques décrits plus haut.

L'atout clé de Norton Mobile Security est la fonction App Advisor.

Alimenté par Norton Mobile Insight, App Advisor vous apporte une protection proactive en vous permettant d'analyser les applications sur Google Play AVANT leur téléchargement (sur Android version 4.0 et ultérieure, ou Android version 4.2 et ultérieure sur les appareils Samsung). La fonction vous indique si les applications contiennent du code malveillant, risquent de porter atteinte à votre vie privée ou consomment beaucoup de batterie et de données. De la même façon, elle analyse automatiquement les applications Android déjà téléchargées ou installées sans passer par une plate-forme de téléchargement et vous propose de les supprimer.

En une seule opération simple, vous pouvez faire des choix en connaissance de cause et décider quelle application vaut le risque d'être conservée.

Norton Mobile Security propose également d'autres composants de protection proactive pour vous et vos appareils Android, comme la protection Web, véritable bouclier contre les sites frauduleux conçus pour subtiliser vos informations et votre argent, ou encore un outil de récupération à distance qui vous aidera à retrouver votre appareil Android, iPhone ou iPad plus rapidement. Vous pouvez même sauvegarder vos contacts et les récupérer en cas de perte ou de vol. Il est désormais facile de protéger tous vos appareils avec un même service Web proposé en abonnement. Avec Norton Mobile Security, vous profitez de la liberté et du confort des appareils mobiles en toute sécurité.

Avancez confiant avec la solution Norton

La mobilité fait partie intégrante de votre vie quotidienne. Mais plus vous vous reposez sur ces petits ordinateurs que sont vos appareils mobiles, plus il est urgent de discerner les risques de sécurité et d'agir pour vous en protéger.

Les technologies de protection mobile Norton sont également disponibles dans nos produits multiplateformes Norton Security et Norton Security avec Backup.

Que ce soit pour vous, ou votre famille, ces abonnements vous apportent une protection sur mesure pour vos PC et Mac ainsi que vos appareils Android et iOS avec une solution complète et facile à utiliser, en tous lieux et à tout moment.

Rendez-vous sur Google Play™ pour tester, gratuitement et pendant 30 jours, toutes les fonctions de protection avancée de l'abonnement Norton Mobile Security Premium. Il vous suffit de créer un compte Norton ; aucun numéro de carte bancaire ne vous sera demandé. À l'issue de la période d'essai, vous pourrez passer à l'abonnement Premium payant ou continuer à utiliser les fonctions gratuites.