Top des risques de sÃ©curitÃ© des applications mobiles
MobilitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 8/1/2024 13:00:00

Ces derniÃ¨res annÃ©es, en particulier avec le travail hybride, presque tout le monde utilise un appareil iOS ou AndroÃ¯d pour le travail.

Dans une enquÃªte rÃ©cente, Lookout, partenaire cybersÃ©curitÃ© de Betoobe, a constatÃ© que 92 % des collaborateurs travaillant Ã distance utilisent leur ordinateur portable ou leur smartphone personnel pour effectuer des tÃ¢ches professionnelles, et que 46 % d'entre eux ont sauvegardÃ© des fichiers professionnels sur ces appareils.

Maintenant que les collaborateurs s'attendent Ã pouvoir Ãªtre productifs depuis n'importe quel endroit, les organisations de tous les secteurs sont devenues plus dÃ©tendues et autorisent dÃ©sormais l'utilisation d'appareils personnels dans le cadre de programmes BYOD (Bring Your Own Device) ou le COPE (Company Owned, Personnaly Enabled), tout comme la connexion aux diffÃ©rents services de lâ□□entreprise Ã travers une diversitÃ© de rÃ©seaux internet.

Avec ces changements fondamentaux, si les appareils mobiles ne sont pas considÃ©rÃ©s comme une partie importante de la stratÃ©gie globale de sÃ©curitÃ© et de gestion des risques, ils prÃ©sentent une vulnÃ©rabilitÃ© pour n'importe quelle organisation.

Ã□tant donnÃ© que les collaborateurs peuvent accÃ©der Ã une multitude de donnÃ©es d'entreprise Ã partir de leurs appareils mobiles, il est essentiel de comprendre comment le fait d'autoriser les appareils mobiles professionnels et/ou personnels peut affecter le risque global, en particulier lorsqu'il s'agit d'applications personnelles dont les permissions peuvent mettre en danger vos collaborateurs, leurs appareils et les donnÃ©es (personnelles et professionnelles) auxquelles ils ont accÃ¨s.

Les applications peuvent Ãªtre dangereuses sans Ãªtre malveillantes

La plateforme de mÃ©dias sociaux chinoise TikTok est un exemple trÃ¨s mÃ©diatisÃ© d'application Ã risque qui a fait son apparition. Alors que les gouvernements du monde entier se sont concentrÃ©s sur l'interdiction de TikTok, leurs prÃ©occupations concernant l'accÃ¨s aux donnÃ©es et la connexion avec la Chine pourraient s'appliquer Ã des milliers d'applications que nous utilisons tous.

Ainsi, le cas de TikTok montre qu'une application qui n'est pas fonciÃ¨rement malveillante peut tout de mÃªme prÃ©senter un risque pour les donnÃ©es des organisations. Mais ce nâ□□est quâ□□un exemple parmi tant dâ□□autres qui illustre Ã quel point les applications personnelles peuvent Ãªtre dangereuses en raison des donnÃ©es qu'elles collectent.

Qu'il s'agisse d'une question de sÃ©curitÃ© nationale, comme le revendiquent de nombreux organismes gouvernementaux en AmÃ©rique du Nord et en Europe, ou d'une question de conformitÃ© aux lois telles que le RGPD, il est essentiel de comprendre comment les applications mobiles peuvent potentiellement accÃ©der Ã des donnÃ©es sensibles et les manipuler.

Des fonctionnalitÃ©s malveillantes peuvent Ãªtre cachÃ©es dans des applications lÃ©gitimes

Outre TikTok, de rÃ©centes dÃ©couvertes concernant la populaire application chinoise de commerce Ã©lectronique Pinduoduo ont dÃ©montrÃ© que des fonctionnalitÃ©s malveillantes peuvent Ãªtre dissimulÃ©es dans des applications dÃ©veloppÃ©es par des organisations lÃ©gitimes.

Pinduoduo a Ã©tÃ© retirÃ©e de Google Play aprÃ¨s que des chercheurs ont dÃ©couvert que ses versions off-store, principalement utilisÃ©es pour le marchÃ© chinois, pouvaient exploiter des vulnÃ©rabilitÃ©s de type "zero-day" et prendre le contrÃ´le d'appareils de diverses maniÃ¨res.

AprÃ¨s l'annonce concernant Pinduoduo (PDD), les chercheurs du Lookout Threat Lab ont dÃ©cidÃ© de se pencher sur Temu, une autre application e-commerce trÃ¨s populaire dÃ©veloppÃ©e par la mÃªme sociÃ©tÃ© mÃ¨re :

â¢ L'Ã©quipe Lookout a dÃ©couvert que du code dans Temu avait Ã©tÃ© supprimÃ© aprÃ¨s la dÃ©couverte de Pinduoduo
â¢ Plus inquiÃ©tant encore, les versions 1.55.2 et antÃ©rieures disposaient d'une capacitÃ© de correction par le biais d'un outil maison connu sous le nom de "Manwe", un outil de dÃ©compression et de correction qui a Ã©galement Ã©tÃ© dÃ©couvert dans les versions malveillantes de Pinduoduo
â¢ Manwe pourrait permettre aux dÃ©tenteurs de PDD de corriger l'application sur l'appareil, plutÃ´t que par l'intermÃ©diaire de l'App Store d'Apple ou du Play Store de Google, une pratique qui va Ã l'encontre des politiques des stores d'applications, car elle pourrait permettre au dÃ©veloppeur de diffuser des codes non autorisÃ©s via des mises Ã jour sur les appareils des utilisateurs

Bien qu'aucun fichier exÃ©cutable n'ait Ã©tÃ© transmis par l'intermÃ©diaire de Manwe (ce qui aurait indiquÃ© une utilisation malveillante), le mÃªme code existait dans les versions de Pinduoduo qui ont Ã©tÃ© jugÃ©es malveillantes en raison de cette fonctionnalitÃ©.

Au vu de lâutilisation de cette fonctionnalitÃ© pour exÃ©cuter des activitÃ©s malveillantes dans une autre application de la sociÃ©tÃ© mÃ¨re, il est donc risquÃ© dâavoir dâanciennes versions de Temu sur des appareils mobiles. Lookout recommande par consÃ©quent de ne pas utiliser les versions 1.55.2 et antÃ©rieures de Temu et suggÃ¨re que les administrateurs considÃ¨rent ceci comme faisant partie de leur stratÃ©gie de tolÃ©rance au risque.

Outre ces recommandations, il est important de garder en tÃªte que des applications lÃ©gitimes, dÃ©veloppÃ©es par des organisations lÃ©gitimes, peuvent comporter des fonctionnalitÃ©s malveillantes.

Comment limiter les risques liÃ©s aux applications mobiles

La visibilitÃ© des risques liÃ©s aux applications mobiles peut constituer un dÃ©fi de taille, nÃ©anmoins rÃ©alisable, surtout si, comme la plupart des entreprises, le parc d'appareils se compose d'iOS, d'Android, d'appareils gÃ©rÃ©s et d'appareils non gÃ©rÃ©s. De plus, compte tenu de la configuration des systÃ¨mes d'exploitation mobiles, il est trÃ¨s difficile d'analyser manuellement les applications Ã la recherche de codes malveillants.

Qu'il s'agisse de s'attaquer aux vulnÃ©rabilitÃ©s au niveau du systÃ¨me d'exploitation mobile, aux risques liÃ©s aux applications comme ceux dÃ©crits ci-dessus ou aux menaces de phishing et de rÃ©seau, la sÃ©curitÃ© mobile est essentielle Ã la sÃ©curitÃ© de toute organisation.

Voici trois Ã©lÃ©ments clÃ©s Ã prendre en compte pour mieux surveiller et attÃ©nuer ces menaces :

1. Penser au-delÃ de la gestion de flotte IT : les solutions de gestion des appareils mobiles (MDM)

sont trÃ¨s utiles, mais ce n'est pas pour rien qu'on les appelle des outils de gestion et non des outils de sÃ©curitÃ©. En ce qui concerne les risques liÃ©s aux applications, les solutions de gestion des appareils mobiles ont un certain contrÃ´le sur les applications installÃ©es par les utilisateurs, mais elles n'ont aucune visibilitÃ© sur les risques eux-mÃªmes.

2. Effectuer une surveillance continue basÃ©e sur les risques : pour minimiser les risques, il faut avoir une visibilitÃ© en temps rÃ©el sur l'application elle-mÃªme, notamment sur les autorisations dont elle dispose, la maniÃ¨re dont les donnÃ©es sont traitÃ©es, les rÃ©seaux avec lesquels elle communique, les vulnÃ©rabilitÃ©s et les codes malveillants qui y sont intÃ©grÃ©s.

3. Appliquer les politiques de faÃ§on cohÃ©rente : de nombreuses solutions de sÃ©curitÃ© des terminaux mobiles sont limitÃ©es dans les protections qu'elles peuvent fournir Ã certains types d'appareils, ce qui peut entraÃ®ner des lacunes qui compromettent les appareils, les utilisateurs ainsi que les donnÃ©es.

Une vÃ©ritable solution de dÃ©fense contre les menaces mobiles devrait permettre d'appliquer les politiques et les protections de maniÃ¨re cohÃ©rente sur tous les appareils, qu'il s'agisse d'appareils iOS ou Android, de smarthpones ou dâ□□ordinateurs ou autres appareils informatiques, quâ□□ils soient gÃ©rÃ©s en COBO (Company Owned, Business Only), en COPE (company-owned, personally enabled) ou en BYOD (Bring your own device).

Compte tenu du rÃ´le indÃ©niablement prÃ©pondÃ©rant des appareils informatiques dans les habitudes de travail actuelles, les risques liÃ©s aux applications mobiles ne peuvent pas Ãªtre ignorÃ©s, quelle que soit la taille ou la configuration de lâ□□organisation, dixit SÃ©bastien REVERDY chez Betoobe.